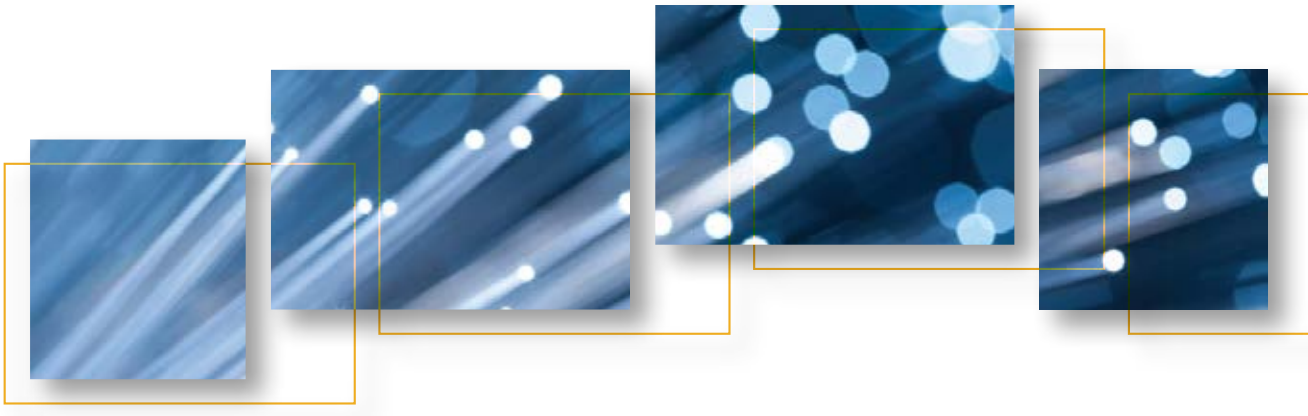
Australian Government
Attorney-General's Department

# TELECOMMUNICATIONS (INTERCEPTION AND ACCESS) ACT 1979

## Annual Report 2013–14



# TELECOMMUNICATIONS (INTERCEPTION AND ACCESS) ACT 1979

**Annual Report 2013–14**

ISBN 978-1-925118-83-4



Contact us

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

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

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

# CONTENTS


EXECUTIVE SUMMARY V

CHAPTER 1 – TELECOMMUNICATIONS INTERCEPTION 1

- Key legislative developments 2013–14 1
- Key judicial decisions 2013–14 2
- Key policy developments 2013–14 3
- Serious offences 5
- Eligibility to issue an interception warrant 7
- Applications for and issue of telecommunications interception warrants 7
- Effectiveness of telecommunications interception warrants 12
- Named person warrants 16
- B-Party warrants 20
- Duration of warrants 21
- Eligible warrants 24
- Interception without a warrant 25
- Mutual assistance 26
- Number of interceptions carried out on behalf of other agencies 26
- Telecommunications interception expenditure 27
- Emergency service facilities 28
- Safeguards, controls and reporting requirements 29
- Commonwealth Ombudsman—inspection of telecommunications interception records 30
- Commonwealth Ombudsman's summary of findings 31
- Commonwealth Ombudsman's findings for individual agency 31

CHAPTER 2 – STORED COMMUNICATIONS 35
Effectiveness of stored communications warrants 37
Preservation notices 38
Mutual assistance 39
Commonwealth Ombudsman—inspection of stored communications access records 40
CHAPTER 3 – TELECOMMUNICATIONS DATA44
Existing data—enforcement of a criminal law 45
Existing data—enforcement of a law imposing a pecuniary penalty or protecting public revenue 48
Prospective data—authorisations 52
Data authorisations to locate missing persons 53
Data authorisations for foreign law enforcement 54
CHAPTER 4 – FURTHER INFORMATION 55
APPENDIX A – LIST OF TABLES AND FIGURES 56
APPENDIX B – INTERCEPTION AGENCIES UNDER THE TIA ACT 59
APPENDIX C – ABBREVIATIONS 60
APPENDIX D – CATEGORIES OF SERIOUS OFFENCES 62

# EXECUTIVE SUMMARY

The *Telecommunications (Interception and Access) Act 1979 Act Annual Report 2013–14* sets out how eligible Commonwealth, State and Territory government agencies have used the powers available under the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) between 1 July 2013 and 30 June 2014.

The primary function of the TIA Act is to protect the privacy of the communications of people who use the Australian telecommunications network. Law enforcement agencies'[1] use of interception powers under the TIA Act is independently overseen by the Commonwealth Ombudsman and equivalent state bodies.

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.

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.

## Legislative reforms

This 2013–14 annual report contains reports on three 'eligible authorities'[2] under the TIA Act created by an amendment to the TIA Act during the 2012–13 reporting period. These new eligible authorities are the Independent Broad-based Anti-corruption Commission (Victoria), the Victorian Inspectorate, and the Independent Commissioner Against Corruption (South Australia).

## Key judicial decisions

This 2013–14 annual report contains two decisions from courts in South Australia and Western Australia. These decisions relate to provisions in the TIA Act dealing with notifying a carrier of the issue of a warrant and exempt proceedings.

---

1 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.

2 Eligible authorities can access information obtained under telecommunications interception warrants and can be declared by the Commonwealth Attorney-General to be an interception agency (subject to being satisfied that the requesting State has met the preconditions in section 35 of the TIA Act).

## Policy developments

There were two inquiries during the 2013–14 reporting period:

- the Senate Legal and Constitutional Affairs Reference Committee Inquiry into a comprehensive revision of the TIA Act with regard to two particular recommendations[3]
- the Senate Legal and Constitutional Affairs Legislation Committee Inquiry into the Telecommunications Amendment (Get a Warrant) Bill 2013.

## Key findings

- In 2013–14, issuing authorities issued 4,007 interception warrants, a decrease of around 5 per cent from 2012–13, when 4,232 warrants were issued. Interception warrants are highly privacy intrusive and are only sought when operationally necessary.
- During 2013–14, information obtained under interception warrants was used in:[4]
  - 2,938 arrests
  - 4,008 prosecutions
  - 2,210 convictions.
- In 2013–14, 77 enforcement agencies made 334,658 authorisations for the disclosure of historical telecommunications data. Of these, 324,260 authorisations were made to enforce a criminal law. This compares with 330,798 data authorisations made by 73 enforcement agencies in 2012–13, of which 320,032 authorisations were made to enforce a criminal law (a 1.3 per cent increase from 2012–13). A total increase of 1.2 per cent is significantly less than the previous reporting period. In 2012–13 around 9.8 per cent more authorisations were made than in 2011–12.
- In 2013–14, 139 B-Party warrants[5] were issued, around 16 per cent more than in 2012–13. Around 10 per cent of these warrants were issued with conditions or restrictions.
- In 2013–14, 999 named person warrants were issued, a 12 per cent increase from 2012–13. The increase is consistent with fluctuations associated with operational demand (between 2011–12 and 2012–13 there was a 28 per cent increase in the number of named person warrants issued).

---

3 a. the recommendations of the Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* report, dated May 2008, particularly recommendation 71.2; and b. recommendations relating to the Act from the Parliamentary Joint Committee on Intelligence and Security *Inquiry into the potential reforms of Australia's National Security Legislation report*, dated May 2013.

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

5 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.

- In 2013–14, law enforcement agencies made 153 arrests, conducted 176 prosecutions and obtained 144 convictions based on evidence obtained under stored communications warrants.[6]
- In 2013–14, consistent with the last reporting period, the majority of named person warrants were for the interception of between two to five telecommunications services.
- 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.

## Telecommunications interception

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 and, under the TIA Act, can only occur under an interception or stored communications warrant, or in certain limited circumstances such as a life-threatening emergency. Interception is subject to significant limitations, oversight and reporting obligations and the annual report is an important part of this accountability framework.

Lawful interception is an effective investigative tool that supports and complements information obtained through other methods. In many 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 introduced into evidence.

## Telecommunications data

A critical tool available under the TIA Act is access to telecommunications data.[7]

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 criminals being investigated.

Data gives agencies a clear method for tracing all telecommunications from end-to-end and 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).

---

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

7 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.

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. 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.

Under the TIA Act, all enforcement agencies can access historical data[8] and criminal law-enforcement agencies can also access prospective data[9].

This annual report is organised into three main chapters: chapter 1 focuses on interception warrants, chapter 2 reports on stored communications, and chapter 3 deals with telecommunications data.

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

8 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.

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

# 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 and is limited to agencies such as the Australian Federal Police and state police forces eligible to apply under Part 2–5 of the TIA Act for an interception warrant.**

## Key legislative developments 2013–14

### New interception agencies under the TIA Act

In the 2012–13 reporting period, the *Telecommunications Interception and Other Legislation Amendment (State Bodies) Act 2012* (the TI State Bodies Act) amended the TIA Act to add the following agencies as 'eligible authorities' under the TIA Act:

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

Eligible authorities can access information obtained under telecommunications interception warrants and can be declared by the Commonwealth Attorney-General to be an interception agency (subject to being satisfied that the requesting State has met the preconditions in section 35 of the TIA Act).

The IBAC became an interception agency on 10 February 2013, when it replaced the Victorian Office of Police Integrity. The 2013–14 Annual Report contains the first full year of reporting information about the IBAC. The ICAC (SA) became an interception agency on 1 September 2013 and information in this annual report about the ICAC (SA) relates to that time period. Consistent with powers available to other state oversight bodies, the Victorian Inspectorate is not an interception agency.

## Key judicial decisions 2013–14

### Notification of the issue of a warrant

In *R v Scarpantoni (No 2)* [2013] SADC 70 (22 May 2013), the District Court of South Australia followed the reasoning of the Western Australia Court of Appeal in *Geldert v The State of Western Australia* [2012] WASCA 226 (9 November 2012) that, where there is a valid warrant, there is no requirement for the service of a certified copy of the warrant to be a precondition to the agency's authority to commence interception. Notification to the carrier is the means by which the carrier can commence doing what it is required to do to facilitate the interception of the communications by the officers of the agency.

The court found, provided that the carrier has been informed of the issue of the warrant, the carrier did not also require the certified copy in order to commence the interception. The requirement to provide a certified copy of the warrant was to provide an audit trail and underpinned the accountability and reporting obligations in the Act, rather than a necessary part of notification to the carrier.

*Geldert v The State of Western Australia* [2012] WASCA 226 (9 November 2012) rejected the judgments in *The State of Western Australia v Tanevski [No 5]* [2012] WADC 64 (*Tanevski No 1*) and *The State of Western Australia v Tanevski* [2012] WADC 87 (*Tanevski No 2*). In those cases, the WA District Court of Western Australia considered the notification and authorisation provisions in relation to stored communications warrants (sections 121 and 126) and telecommunications service warrants (sections 47 and 60) respectively. The court held that the process for notifying a carrier of a stored communications (*Tanevski No 1*) or interception warrant (*Tanevski No 2*) required the agency to provide a certified copy, in addition to informing the carrier of the warrant.

### Exempt proceedings

In *Sands v State of South Australia* [2013] SASC 44, the Supreme Court of South Australia determined that certain intercepted conversations were admissible in a claim for defamation as the proceeding related to the 'alleged misbehaviour, or alleged improper conduct, of an officer of the Commonwealth or of a State'.

The defamation claim in *Sands* was based on an allegation that the police had acted unlawfully, maliciously and in breach of their statutory duties in the course of the investigation by leaking information to a journalist that identified the plaintiff as the primary murder suspect.

The Supreme Court distinguished the narrower construction in *Kizon v Palmer* (1997) 72 FCR 409, which found that a proceeding relating to 'alleged misbehaviour, or alleged improper conduct, of an officer of the Commonwealth or of a State' referred to alleged misbehaviour or improper conduct of a kind commonly associated with disciplinary action against an employee or office-holder, such as dismissal, removal from office or other sanction.

The Court found that amendments to the definition of 'exempt proceeding' in section 5B of the TIA Act, which were made after the *Kizon* decision, together with the phrase 'any other proceeding' in subsection 5B(1)(f), brought the current proceedings within the TIA Act. The foundation of the defamation claim was that the police acted unlawfully,

maliciously and in breach of their statutory duty, allegations that could lead to disciplinary or criminal charges.

The Court also considered that the intercepted conversations were admissible on the basis that the material had previously been admitted in an earlier proceeding. Under the TIA Act, lawfully intercepted information that has been given in evidence in a previous proceeding can subsequently be given in evidence in any proceeding (section 75A of the TIA Act).

## Key policy developments 2013–14

### Senate inquiry into the *Telecommunications (Interception and Access) Act 1979*

On 12 December 2013, the Senate referred the following matter to the Legal and Constitutional Affairs References Committee (the References Committee) for inquiry and report:

> Comprehensive revision of the *Telecommunications (Interception and Access) Act 1979* (the Act), with regard to:
>
> a. the recommendations of the Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* report, dated May 2008, particularly recommendation 71.2; and
>
> b. recommendations relating to the Act from the Parliamentary Joint Committee on Intelligence and Security *Inquiry into the potential reforms of Australia's National Security Legislation* report, dated May 2013.

The Attorney-General's Department made a submission to the inquiry, a copy of which can be found online at <www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/Comprehensive_revision_of_TIA_Act>

In its submission, the department welcomed the current inquiry and reiterated the relevance of the issues raised by the department in its submission to the 2012–13 *Inquiry into Potential Reforms of Australia's National Security Legislation* by the Parliamentary Joint Committee on Intelligence and Security (the PJCIS).

The References Committee released its report on 24 March 2015, a copy of which can be found online at <www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/Comprehensive_revision_of_TIA_Act>

### Senate inquiry into the Telecommunications Amendment (Get a Warrant) Bill 2013

On 20 June 2013, the Senate referred the Telecommunications Amendment (Get a Warrant) Bill 2013 (the Bill) to the Senate Legal and Constitutional Affairs Legislation Committee (the Legislation Committee) for inquiry and report by 31 October 2013.

The Bill sought to amend the TIA Act to require law enforcement and national security agencies to obtain a warrant to access telecommunications data.

The Legislation Committee received 18 submissions from government agencies and community organisations. The Attorney-General's Department made a submission to the inquiry, a copy of which can be found online at <www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/Completed_inquiries/2010-13/getawarrant2013/submissions>

The department's submission noted that, if enacted, the Bill would significantly affect the ability of law enforcement and national security agencies to perform their legislated roles.

On 5 August 2013, the Governor-General prorogued the 43rd Parliament and dissolved the House of Representatives (a Federal election was held on 7 September 2013). On 20 August 2013 the Legislation Committee wrote to the President of the Senate advising that, consistent with the general approach adopted by other Senate committees to inquiries during elections, the Legislation Committee had resolved not to continue its inquiry into the Bill.

## 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/>

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

During the reporting period interception warrants were only 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.

In the 2013 report *Organised Crime in Australia*, the Australian Crime Commission (the ACC) assessed the overall risk to Australia from organised crime as high[10] and estimated the cost to Australia of organised crime such as identity crime, money laundering, fraud, cybercrime, drug trafficking and people smuggling at $15 billion per year.[11]

The information provided in Table 1 illustrates the important role telecommunications interception plays in investigating serious crimes. Consistent with previous years, in 2013–14 agencies obtained the majority of warrants to assist with investigations into serious drug offences (1,772 warrants). Loss of life or personal injury offences were specified in 624 warrants and 447 warrants related to murder investigations. Organised crime was specified as an offence in 246 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.

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

11 ACC, *Organised Crime in Australia 2013*, p. 6.

**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) | ICAC (NSW) | NSW CC | NSW POL | NT POL | PIC | QLD POL | SA POL | TAS POL | VIC POL | WA POL | IBAC | ICAC (SA) | TOTAL |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ACC special investigations | 235 | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | **235** |
| Administration of Justice | - | - | 2 | - | - | - | - | - | - | - | - | - | - | - | - | - | - | **2** |
| Assisting a person to escape or dispose of proceeds | - | - | - | - | - | - | 12 | 19 | - | - | 12 | - | - | - | - | - | - | **43** |
| Bribery or corruption; offences against ss 131.1, 135.1, 142.1, 142.2, 148.2, 268.112 of the Criminal Code | - | 37 | 21 | 60 | 12 | 21 | - | 5 | - | 29 | - | 1 | - | 2 | 13 | 13 | 6 | **220** |
| Cartel offences | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | **-** |
| Child pornography offences | - | - | 3 | - | - | - | - | 5 | - | - | - | - | - | - | - | - | - | **8** |
| Conspire/aid/abet serious offence | - | - | 10 | - | - | - | 5 | 38 | - | 2 | - | 7 | - | - | - | - | - | **62** |
| Cybercrime offences | - | - | 3 | 4 | - | - | - | 1 | - | - | - | - | - | - | - | - | - | **8** |
| Kidnapping | - | - | 9 | - | - | - | 3 | 32 | - | - | - | - | - | 9 | 1 | - | - | **54** |
| Loss of life or personal injury | - | - | 46 | - | 2 | - | 3 | 469 | 3 | - | 29 | 9 | - | 46 | 17 | - | - | **624** |
| Money laundering | 15 | - | 151 | - | - | - | 41 | 4 | - | - | - | 1 | - | 1 | 18 | - | - | **231** |
| Murder | - | - | 12 | - | - | - | 51 | 180 | 7 | - | 51 | 43 | 9 | 59 | 35 | - | - | **447** |
| Organised offences and/or criminal organisations | - | - | 7 | - | - | - | 16 | 186 | - | - | 1 | - | - | 1 | 35 | - | - | **246** |
| People smuggling and related | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | **-** |
| Serious damage to property and/or serious arson | - | - | 28 | - | - | - | - | 55 | - | - | 4 | - | 2 | 3 | 13 | - | - | **105** |
| Serious drug offences and/or trafficking | 3 | 2 | 493 | - | 24 | - | 230 | 462 | 33 | 4 | 207 | 68 | 24 | 55 | 167 | - | - | **1,772** |
| Serious fraud and/or revenue loss | - | - | 24 | - | - | - | - | 52 | - | - | - | 1 | - | - | 1 | 3 | - | **81** |
| Telecommunications offences | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | **-** |
| Terrorism offences | - | - | 152 | - | - | - | - | 6 | - | - | - | - | - | - | - | - | - | **158** |
| **Total** | **253** | **39** | **961** | **64** | **38** | **21** | **361** | **1,514** | **43** | **35** | **304** | **130** | **35** | **176** | **300** | **16** | **6** | **4,296** |

## 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 shows that in 2013–14 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
- 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 | 11 |
| Family Court judges | 7 |
| Federal Circuit Court judges | 33 |
| Nominated AAT members | 29 |

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

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

## Applications for and issue of telecommunications interception warrants

Tables 3 and 4 set out information about the number of eligible judges and nominated AAT members and the agencies to which they issued warrants. In 2013–14, issuing authorities issued 4,007 interception warrants, a decrease of around 5 per cent from 2012–13, when 4,232 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 | - | 2 | 17 | 234 |
| ACLEI | - | - | 20 | 5 |
| AFP | 13 | 105 | 56 | 510 |
| CCC (WA) | 7 | - | - | 57 |
| CCC (QLD) | - | - | 3 | 35 |
| ICAC (NSW) | - | - | - | 21 |
| NSW CC | - | - | - | 349 |
| NSW Police | - | - | 105 | 1,409 |
| NT Police[12] | - | - | 23 | 20 |
| PIC | - | - | - | 35 |
| QLD Police | - | - | 227 | 77 |
| SA Police[13] | - | 6 | 15 | 111 |
| TAS Police | - | - | - | 35 |
| VIC Police | - | - | - | 188 |
| WA Police | 196 | - | - | 104 |
| IBAC | - | - | - | 16 |
| ICAC (SA) | - | - | - | 6 |
| **Total** | **216** | **113** | **466** | **3,212** |

12 NT Police has advised the Attorney-General's Department that the 2012–13 report should be revised to note that 21 warrants were issued by AAT members, 2 warrants were issued by Federal Court judges and 48 by Federal Circuit judges.

13 SA Police has advised the Attorney-General's Department that the 2012–13 Report should be revised to note that 124 warrants were issued by AAT members, 1 warrant was issued by a Federal Court judge and 1 warrant was issued by a Federal Circuit Court judge.

**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[14] | | Renewal applications[15] | |
|---|---|---|---|---|---|---|---|
| | | 12/13 | 13/14 | 12/13 | 13/14 | 12/13 | 13/14 |
| ACC | Made | 195 | 253 | - | - | 36 | 25 |
| | Refused/withdrawn | - | - | - | - | - | - |
| | Issued | 195 | 253 | - | - | 36 | 25 |
| ACLEI | Made | 10 | 25 | - | - | 3 | 17 |
| | Refused/withdrawn | - | - | - | - | - | - |
| | Issued | 10 | 25 | - | - | 3 | 17 |
| AFP | Made | 640 | 690 | - | - | 149 | 143 |
| | Refused/withdrawn | 6 | 6 | - | - | - | - |
| | Issued | 634 | 684 | - | - | 149 | 143 |
| CCC (WA) | Made | 17 | 67 | - | - | - | 23 |
| | Refused/withdrawn | - | 3 | - | - | - | - |
| | Issued | 17 | 64 | - | - | - | 23 |
| CCC (QLD) | Made | 26 | 38 | - | - | 2 | 7 |
| | Refused/withdrawn | - | - | - | - | - | - |
| | Issued | 26 | 38 | - | - | 2 | 7 |
| ICAC (NSW) | Made | 5 | 21 | - | - | 1 | 8 |
| | Refused/withdrawn | - | - | - | - | - | - |
| | Issued | 5 | 21 | - | - | 1 | 8 |
| NSW CC | Made | 417 | 349 | - | - | 105 | 71 |
| | Refused/withdrawn | 1 | - | - | - | - | - |
| | Issued | 416 | 349 | - | - | 105 | 71 |
| NSW Police | Made | 1,846 | 1,519 | 70 | 57 | 182 | 197 |
| | Refused/withdrawn | 7 | 5 | 1 | - | - | - |
| | Issued | 1,839 | 1,514 | 69 | 57 | 182 | 197 |
| NT Police | Made | 71 | 43 | - | - | 2 | 4 |
| | Refused/withdrawn | - | - | - | - | - | - |
| | Issued | 71 | 43 | - | - | 2 | 4 |
| PIC | Made | 70 | 35 | - | - | 35 | 8 |
| | Refused/withdrawn | - | - | - | - | - | - |
| | Issued | 70 | 35 | - | - | 35 | 8 |
| QLD Police | Made | 292 | 308 | - | - | 36 | 33 |
| | Refused/withdrawn | - | 4 | - | - | - | - |
| | Issued | 292 | 304 | - | - | 36 | 33 |

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

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

| Agency | Relevant statistics | Applications for warrants | | Telephone applications for warrants[14] | | Renewal applications[15] | |
|---|---|---|---|---|---|---|---|
| | | 12/13 | 13/14 | 12/13 | 13/14 | 12/13 | 13/14 |
| SA Police[16] | Made | 126 | 132 | - | 3 | 6 | 9 |
| | Refused/withdrawn | - | - | - | - | - | - |
| | Issued | 126 | 132 | - | 3 | 6 | 9 |
| TAS Police | Made | 23 | 35 | - | - | 1 | 6 |
| | Refused/withdrawn | - | - | - | - | - | - |
| | Issued | 23 | 35 | - | - | 1 | 6 |
| VIC Police | Made | 233 | 188 | 19 | 15 | 21 | 7 |
| | Refused/withdrawn | 1 | - | - | - | - | - |
| | Issued | 232 | 188 | 19 | 15 | 21 | 7 |
| WA Police | Made | 276 | 300 | 1 | - | 28 | 44 |
| | Refused/withdrawn | - | - | - | - | - | - |
| | Issued | 276 | 300 | 1 | - | 28 | 44 |
| IBAC | Made | - | 16 | - | - | - | 1 |
| | Refused/withdrawn | - | - | - | - | - | - |
| | Issued | - | 16 | - | - | - | 1 |
| ICAC (SA) | Made | - | 6 | - | - | - | - |
| | Refused/withdrawn | - | - | - | - | - | - |
| | Issued | - | 6 | - | - | - | - |
| **Total** | **Made** | **4,247** | **4,025** | **90** | **75** | **607** | **603** |
| | **Refused/withdrawn** | **15** | **18** | **1** | **-** | **-** | **-** |
| | **Issued** | **4,232** | **4,007** | **89** | **75** | **607** | **603** |

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 by less intrusive means. Agencies only use this type of warrant on rare occasions. One warrant was issued in 2013–14 (see Table 5).

16 SA Police has advised the Attorney-General's Department that the 2012–13 figure should be revised up from 121 warrants to 126 warrants.

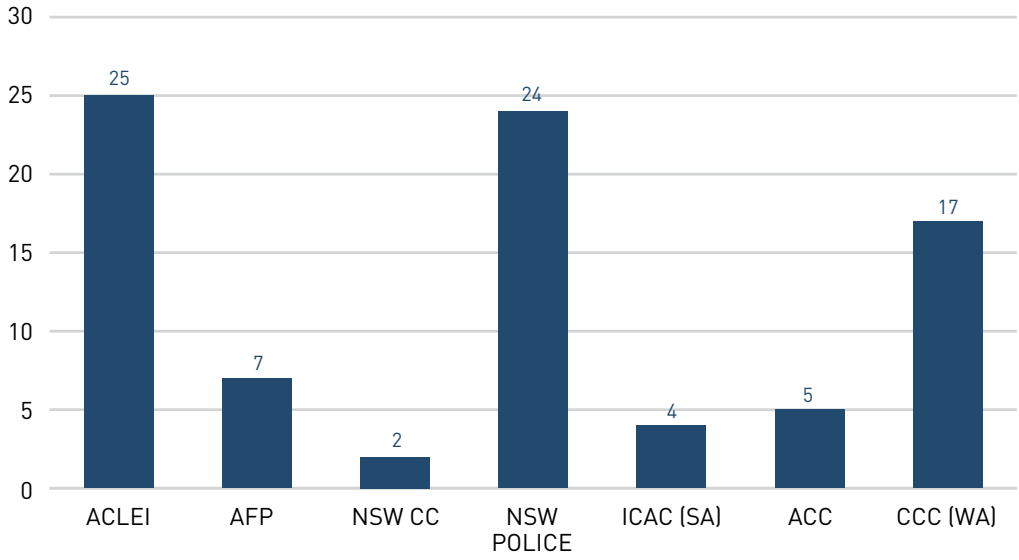
**Table 5: Applications for telecommunications interception warrants authorising entry on premises—ss. 100(1)(d) and 100(2)(d)**

| Agency | Relevant statistics | Warrants authorising entry on premises | |
|---|---|---|---|
| | | 12/13 | 13/14 |
| AFP | Made | 11 | - |
| | Refused/withdrawn | - | - |
| | Issued | 11 | - |
| CCC (WA) | Made | 1 | 1 |
| | Refused/withdrawn | - | - |
| | Issued | 1 | 1 |
| NSW CC | Made | 1 | - |
| | Refused/withdrawn | - | - |
| | Issued | 1 | - |
| **Total** | **Made** | **13** | **1** |
| | **Refused/withdrawn** | **-** | **-** |
| | **Issued** | **13** | **1** |

An issuing authority can place conditions or restrictions on an interception warrant.

Figure 1 provides information about the use of warrants issued with conditions or restrictions. In 2013–14, 84 interception warrants were issued with a condition or a restriction, 25 per cent less than the last reporting period (in 2012–13, 112 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 many 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 introduced into evidence.

In 2013–14 there were 2,938 arrests, 4,008 prosecutions and 2,210 convictions based on lawfully intercepted material.

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

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

| Agency | Arrests | |
|---|---|---|
| | 12/13 | 13/14 |
| ACC | 62 | 105 |
| ACLEI | 6 | 10 |
| AFP | 296 | 209 |
| CCC (WA) | 0 | 1 |
| CCC (QLD) | 32 | 10 |
| NSW CC | 91 | 139 |
| NSW Police | 1,162 | 1,181 |
| NT Police | 58 | 47 |
| PIC | 15 | 50 |
| QLD Police | 537 | 437 |
| SA Police | 109 | 121 |
| TAS Police | 7 | 57 |
| VIC Police | 338 | 254 |
| WA Police | 238 | 317 |
| **Total** | **2,951** | **2,938** |

CASE STUDY:
## CORRUPTION AND CRIME COMMISSION (WA)

CORRUPTION AND CRIME COMMISSION

A former detective sergeant with the Western Australia Police Service (WA Police) has been jailed in what a magistrate described as 'particularly serious' offences relating to breaches of the TIA Act.

In 2013–14, the Corruption and Crime Commission of Western Australia (the Commission) secured multiple convictions against the former officer, including a conviction for contravening the TIA Act's prohibition for communicating interception warrant information.

After a five month investigation by the Commission into offences that occurred between 2008 and 2013, the former officer was charged with a total of 17 offences. These included one count of unlawful dealing in interception warrant information, 15 counts of unlawful use of a restricted-access computer system and one count of supplying an audio-visual recording of an interview. The former officer was charged in August 2013 and sentenced to nine months imprisonment in September 2014.

The officer was involved in a personal relationship with a lawyer to whom he communicated two affidavits: one relating to a telephone interception warrant and the other to a surveillance devices warrant, both of which contained interception warrant information. The lawyer was not involved in the WA Police investigation.

The Deputy Chief Magistrate noted that the disclosure of the interception warrant information had the potential to seriously compromise investigations, as the documents would normally be the subject of a non-disclosure order. In sentencing the former officer to nine months imprisonment for these offences, the Deputy Chief Magistrate acknowledged that any term of imprisonment for a former officer 'would be difficult' but stated that it was the only way to deal with the gravity of the offences.

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

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

| Categories of offences | ACC | ACLEI | AFP | CCC (WA) | CCC (QLD) | ICAC (NSW) | NSW CC | NSW POL | NT POL | QLD POL | SA POL | TAS POL | VIC POL | WA POL | TOTAL |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ACC special investigations | - | - | - | - | - | - | - | - | - | - | - | - | - | - | **-** |
| Administration of Justice | - | - | 1 | - | - | - | - | - | - | - | - | - | - | - | **1** |
| Assisting a person to escape or dispose of proceeds | - | - | - | - | - | - | 1 | 3 | - | - | - | - | 1 | - | **5** |
| Bribery or corruption; offences against ss 131.1, 135.1, 142.1, 142.2, 148.2, 268.112 of the Criminal Code | - | 1 | 9 | 4 | - | - | - | - | - | - | 1 | - | 4 | - | **19** |
| Cartel offences | - | - | - | - | - | - | - | - | - | - | - | - | - | - | **-** |
| Child pornography offences | - | - | 1 | - | - | - | - | 23 | - | - | - | - | - | - | **24** |
| Conspire/aid/abet serious offence | 2 | - | - | - | - | - | - | 26 | - | - | 7 | - | 9 | - | **44** |
| Cybercrime offences | - | - | - | 7 | - | - | - | 8 | - | - | - | - | - | - | **15** |
| Kidnapping | - | - | - | - | - | - | - | 18 | - | - | - | - | 8 | - | **26** |
| Loss of life or personal injury | - | - | 1 | - | - | - | 3 | 175 | - | 5 | 3 | - | 77 | 7 | **271** |
| Money laundering | - | - | 15 | - | - | - | 14 | 3 | - | - | 8 | - | 30 | 8 | **78** |
| Murder | - | - | - | - | - | - | - | 45 | - | 4 | 7 | - | 8 | 12 | **76** |
| Organised offences and/or criminal organisations | - | - | - | - | - | - | 19 | 210 | - | 38 | 10 | - | - | 278 | **555** |
| People smuggling and related | - | - | 6 | - | - | - | - | - | - | - | - | - | - | - | **6** |
| Serious damage to property and/or serious arson | - | - | - | - | - | - | - | 24 | - | 7 | - | - | - | 4 | **35** |
| Serious drug offences and/or trafficking | 9 | 4 | 109 | - | 22 | - | 102 | 1,046 | 1 | 149 | 81 | - | 202 | 505 | **2,230** |
| Serious fraud and/or revenue loss | - | - | 4 | 1 | - | 1 | 2 | 12 | - | - | - | - | - | - | **20** |
| Telecommunications offences | - | - | - | - | - | - | - | 4 | - | - | - | - | - | - | **4** |
| Terrorism offences | - | - | 1 | - | - | - | - | - | - | - | - | - | - | - | **1** |
| Other serious offences | - | - | 43 | 9 | 1 | 6 | - | 284 | 2 | 137 | 10 | - | 106 | - | **598** |
| **Total** | **11** | **5** | **190** | **21** | **23** | **7** | **141** | **1,881** | **3** | **340** | **127** | **-** | **445** | **814** | **4,008** |

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

| Categories of offences | ACC | ACLEI | AFP | CCC (WA) | CCC (QLD) | ICAC (NSW) | NSW CC | NSW POL | NT POL | QLD POL | SA POL | VIC POL | WA POL | TOTAL |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ACC special investigations | - | - | - | - | - | - | - | - | - | - | - | - | - | **-** |
| Administration of Justice | - | - | - | - | - | - | - | - | - | - | - | - | - | **-** |
| Assisting a person to escape or dispose of proceeds | - | - | - | - | - | - | 1 | 2 | - | - | - | 1 | - | **4** |
| Bribery or corruption; offences against ss 131.1, 135.1, 142.1, 142.2, 148.2, 268.112 of the Criminal Code | - | 1 | 4 | 4 | - | - | - | - | - | - | - | 4 | - | **13** |
| Cartel offences | - | - | - | - | - | - | - | - | - | - | - | - | - | **-** |
| Child pornography offences | - | - | - | - | - | - | - | 9 | - | - | - | - | - | **9** |
| Conspire/aid/abet serious offence | - | - | - | - | - | - | - | 7 | - | - | - | 4 | - | **11** |
| Cybercrime offences | - | - | - | 7 | - | - | - | - | - | - | - | - | - | **7** |
| Kidnapping | - | - | - | - | - | - | - | - | - | - | - | 4 | - | **4** |
| Loss of life or personal injury | - | - | - | - | - | - | 3 | 28 | - | 7 | - | 48 | 2 | **88** |
| Money laundering | - | - | 2 | - | - | - | 4 | 2 | - | - | - | 24 | 4 | **36** |
| Murder | - | - | - | - | - | - | - | 7 | - | 2 | 1 | 5 | 4 | **19** |
| Organised offences and/or criminal organisations | - | - | - | - | - | - | 8 | 100 | - | 38 | - | - | 153 | **299** |
| People smuggling and related | - | - | 4 | - | - | - | - | - | - | - | - | - | - | **4** |
| Serious damage to property and/or serious arson | - | - | - | - | - | - | - | 7 | - | 7 | - | - | 2 | **16** |
| Serious drug offences and/or trafficking | 3 | 4 | 21 | - | 22 | - | 75 | 446 | 24 | 149 | 9 | 183 | 321 | **1,257** |
| Serious fraud and/or revenue loss | - | - | 1 | 1 | - | 1 | 2 | 19 | - | - | - | - | - | **24** |
| Telecommunications offences | - | - | - | - | - | - | - | - | - | - | - | - | - | **-** |
| Terrorism offences | - | - | - | - | - | - | - | - | - | - | - | - | - | **-** |
| Other serious offences | - | - | 11 | 9 | 1 | 5 | - | 170 | 3 | 137 | 2 | 81 | - | **419** |
| **Total** | **3** | **5** | **43** | **21** | **23** | **6** | **93** | **797** | **27** | **340** | **12** | **354** | **486** | **2,210** |

## Named person warrants

A named person warrant can authorise the interception of telecommunications services (such as a landline or mobile service), and in certain circumstances, telecommunications devices (such as a mobile handset). Before issuing a named person warrant an issuing authority must take into account:

- how much the privacy of any person would be likely to be interfered with
- the gravity of the offence
- whether the interception will assist in the investigation
- 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 2013–14, 999 named person warrants were issued, a 12 per cent increase from 2012–13. The increase is consistent with fluctuations associated with operational demand (between 2011–12 and 2012–13 there was a 28 per cent increase in the number of named person warrants issued).

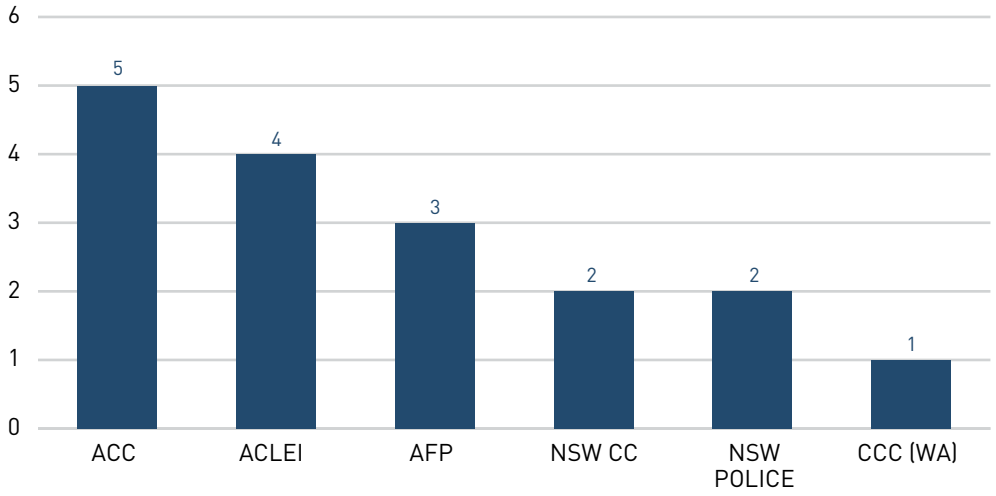
**Table 9: Original applications for named person warrants, telephone applications for named person warrants and renewal applications—ss. 100(1)(ea) and 100(2)(ea)**

| Agency | Relevant statistics | Applications for named person warrants | | Telephone applications for named person warrants | | Renewal applications for named person warrants | |
|---|---|---|---|---|---|---|---|
| | | 12/13 | 13/14 | 12/13 | 13/14 | 12/13 | 13/14 |
| ACC | Made | 124 | 168 | - | - | 30 | 22 |
| | Refused/withdrawn | - | - | - | - | - | - |
| | Issued | 124 | 168 | - | - | 30 | 22 |
| ACLEI | Made | 3 | 4 | - | - | 2 | 1 |
| | Refused/withdrawn | - | - | - | - | - | - |
| | Issued | 3 | 4 | - | - | 2 | 1 |
| AFP | Made | 290 | 318 | - | - | 96 | 106 |
| | Refused/withdrawn | 5 | 3 | - | - | - | - |
| | Issued | 285 | 315 | - | - | 96 | 106 |
| CCC (WA) | Made | 3 | 2 | - | - | - | 1 |
| | Refused/withdrawn | - | - | - | - | - | - |
| | Issued | 3 | 2 | - | - | - | 1 |
| CCC (QLD) | Made | 9 | 13 | - | - | 1 | 6 |
| | Refused/withdrawn | - | - | - | - | - | - |
| | Issued | 9 | 13 | - | - | 1 | 6 |
| NSW CC | Made | 96 | 145 | - | - | 19 | 32 |
| | Refused/withdrawn | - | - | - | - | - | - |
| | Issued | 96 | 145 | - | - | 19 | 32 |

| Agency | Relevant statistics | Applications for named person warrants | | Telephone applications for named person warrants | | Renewal applications for named person warrants | |
|---|---|---|---|---|---|---|---|
| | | 12/13 | 13/14 | 12/13 | 13/14 | 12/13 | 13/14 |
| NSW POLICE | Made | 132 | 105 | - | - | 27 | 25 |
| | Refused/withdrawn | - | - | - | - | - | - |
| | Issued | 132 | 105 | - | - | 27 | 25 |
| NT POLICE | Made | 2 | 3 | - | - | - | - |
| | Refused/withdrawn | - | - | - | - | - | - |
| | Issued | 2 | 3 | - | - | - | - |
| PIC | Made | 3 | - | - | - | 1 | - |
| | Refused/withdrawn | - | - | - | - | - | - |
| | Issued | 3 | - | - | - | 1 | - |
| QLD POLICE | Made | 42 | 42 | - | - | 7 | 6 |
| | Refused/withdrawn | - | 1 | - | - | - | - |
| | Issued | 42 | 41 | - | - | 7 | 6 |
| SA POLICE | Made | 32 | 25 | - | - | 1 | - |
| | Refused/withdrawn | - | - | - | - | - | - |
| | Issued | 32 | 25 | - | - | 1 | - |
| TAS POLICE | Made | 1 | 9 | - | - | 1 | 4 |
| | Refused/withdrawn | - | - | - | - | - | - |
| | Issued | 1 | 9 | - | - | 1 | 4 |
| VIC POLICE | Made | 69 | 44 | 1 | 1 | 8 | 1 |
| | Refused/withdrawn | - | - | - | - | - | - |
| | Issued | 69 | 44 | 1 | 1 | 8 | 1 |
| WA POLICE | Made | 94 | 117 | - | - | 15 | 26 |
| | Refused/withdrawn | - | - | - | - | - | - |
| | Issued | 94 | 117 | - | - | 15 | 26 |
| IBAC | Made | - | 8 | - | - | - | 1 |
| | Refused/withdrawn | - | - | - | - | - | - |
| | Issued | - | 8 | - | - | - | 1 |
| **Total** | **Made** | **900** | **1,003** | **1** | **1** | **208** | **231** |
| | **Refused/withdrawn** | **5** | **4** | **-** | **-** | **-** | **-** |
| | **Issued** | **895** | **999** | **1** | **1** | **208** | **231** |

Under the TIA Act, issuing authorities can issue a warrant with conditions and restrictions about interceptions under the warrant. In 2013–14, 17 named person warrants were issued with a condition or restriction. In 2012–13, 12 named person warrants were issued with conditions or restrictions.

**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 2013–14 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 | |
| | 12/13 | 13/14 | 12/13 | 13/14 | 12/13 | 13/14 | 12/13 | 13/14 |
| ACC | 31 | 47 | 63 | 106 | 20 | 12 | 6 | - |
| ACLEI | - | 2 | 3 | 2 | - | - | - | - |
| AFP | 61 | 44 | 133 | 195 | 27 | 23 | 7 | 2 |
| CCC (WA) | - | - | 1 | 1 | 1 | - | 1 | 1 |
| CCC (QLD) | 1 | 5 | 8 | 6 | - | 2 | - | - |
| NSW CC | 34 | 51 | 57 | 82 | 2 | 8 | 3 | 1 |
| NSW Police | 31 | 29 | 64 | 59 | 11 | 11 | - | - |
| NT Police | - | - | 1 | 1 | 1 | 1 | - | 1 |
| PIC | - | - | - | - | - | - | 3 | - |
| QLD Police | 8 | 8 | 29 | 27 | 3 | 6 | 2 | - |
| SA Police | 5 | 4 | 22 | 18 | 7 | 2 | - | - |
| TAS Police | - | - | - | 7 | - | 2 | 1 | - |
| VIC Police | 11 | 8 | 54 | 32 | 4 | 4 | - | - |
| WA Police | 20 | 33 | 66 | 74 | 8 | 10 | - | - |
| IBAC | - | - | - | 6 | - | 2 | - | - |
| **Total** | **202** | **231** | **501** | **616** | **84** | **83** | **23** | **5** |

In 2013–14, a total of 2,745 telecommunications services were intercepted under service-based named person warrants.

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

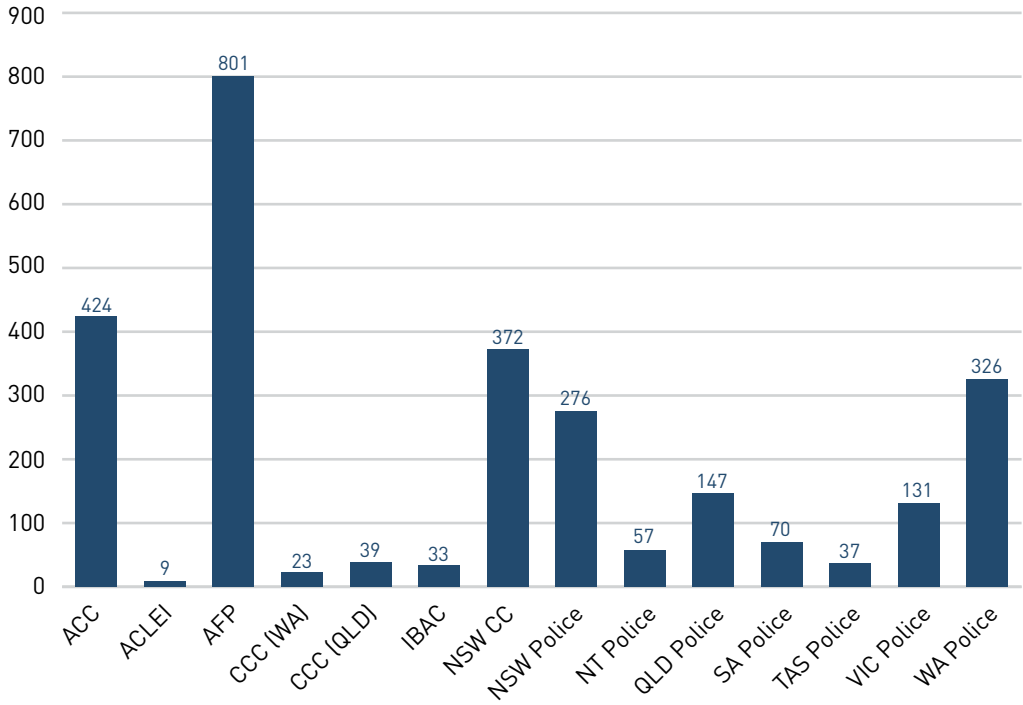



**Table 11: Total number of services and devices intercepted under device-based named person warrants—ss. 100(1)(ec) and 100(2)(ec)**

| Agency | Services | | Devices | |
|---|---|---|---|---|
| | 12/13 | 13/14 | 12/13 | 13/14 |
| ACC | - | - | 17 | 19 |
| AFP | - | - | 66 | 60 |
| NSW CC | - | 1 | 2 | 5 |
| NSW Police | 32 | 10 | 26 | 13 |
| **Total** | **32** | **11** | **111** | **97** |

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 2013–14 device-based named person warrants were used by only a few agencies.

## 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 2013–14, 139 B-Party warrants were issued, around 16 per cent more than in 2012–13. Around 10 per cent of those warrants were issued with conditions on restrictions (see Table 12).

**Table 12: Applications for B-Party warrants, telephone applications for B-Party warrants, and renewal applications—ss. 100(1)(ed) and 100(2)(ed)**

| Agency | Relevant statistics | Applications for B-Party warrants | | Telephone applications for B-Party warrants | | Renewal applications for B-Party warrants | |
|---|---|---|---|---|---|---|---|
| | | 12/13 | 13/14 | 12/13 | 13/14 | 12/13 | 13/14 |
| ACC | Made | 1 | - | - | - | - | - |
| | Refused/withdrawn | - | - | - | - | - | - |
| | Issued | 1 | - | - | - | - | - |
| ACLEI | Made | 2 | 11 | - | - | 1 | 10 |
| | Refused/withdrawn | - | - | - | - | - | - |
| | Issued | 2 | 11 | - | - | 1 | 10 |
| AFP | Made | 34 | 62 | - | - | 21 | 18 |
| | Refused/withdrawn | - | - | - | - | - | - |
| | Issued | 34 | 62 | - | - | 21 | 18 |
| CCC (WA) | Made | 3 | - | - | - | - | - |
| | Refused/withdrawn | - | - | - | - | - | - |
| | Issued | 3 | - | - | - | - | - |
| NSW CC | Made | 1 | 6 | - | - | - | 1 |
| | Refused/withdrawn | - | - | - | - | - | - |
| | Issued | 1 | 6 | - | - | - | 1 |
| NSW Police | Made | 71 | 57 | 20 | 8 | 4 | - |
| | Refused/withdrawn | 1 | - | 1 | - | - | - |
| | Issued | 70 | 57 | 19 | 8 | 4 | - |
| SA Police | Made | - | 3 | - | - | - | 1 |
| | Refused/withdrawn | - | - | - | - | - | - |
| | Issued | - | 3 | - | - | - | 1 |

| Agency | Relevant statistics | Applications for B-Party warrants | | Telephone applications for B-Party warrants | | Renewal applications for B-Party warrants | |
|---|---|---|---|---|---|---|---|
| | | 12/13 | 13/14 | 12/13 | 13/14 | 12/13 | 13/14 |
| QLD Police | Made | 6 | - | - | - | - | - |
| | Refused/withdrawn | - | - | - | - | - | - |
| | Issued | 6 | - | - | - | - | - |
| VIC Police | Made | 2 | - | - | - | - | - |
| | Refused/withdrawn | - | - | - | - | - | - |
| | Issued | 2 | - | - | - | - | - |
| WA Police | Made | 1 | - | - | - | - | - |
| | Refused/withdrawn | - | - | - | - | - | - |
| | Issued | 1 | - | - | - | - | - |
| **Total** | **Made** | **121** | **139** | **20** | **8** | **26** | **30** |
| | **Refused/withdrawn** | **1** | **-** | **1** | **-** | **-** | **-** |
| | **Issued** | **120** | **139** | **19** | **8** | **26** | **30** |

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

| Agency | Applications for B-Party warrants | |
|---|---|---|
| | 12/13 | 13/14 |
| ACLEI | 2 | 11 |
| AFP | 3 | - |
| NSW Police | 1 | 2 |
| **Total** | **6** | **13** |

## 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 | 88 | 51 | 90 | 58 |
| ACLEI | 77 | 62 | 64 | 57 |
| AFP | 80 | 49 | 90 | 74 |
| CCC (WA) | 59 | 48 | 69 | 46 |
| CCC (QLD) | 69 | 60 | 85 | 70 |
| ICAC (NSW) | 86 | 64 | 80 | 57 |
| NSW CC | 53 | 89 | 86 | 71 |
| NSW Police | 67 | 48 | 72 | 56 |
| NT Police | 87 | 56 | 90 | 82 |
| PIC | 70 | 85 | 65 | 62 |
| QLD Police | 61 | 43 | 61 | 56 |
| SA Police | 81 | 63 | 84 | 66 |
| TAS Police | 55 | 46 | 60 | 56 |
| VIC Police | 79 | 56 | 90 | 54 |
| WA Police | 89 | 54 | 90 | 56 |
| ICAC (SA) | 57 | 35 | - | - |
| IBAC | 86 | 72 | 90 | - |
| **Average** | **73** | **58** | **79** | **61** |

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) |
| ACLEI | 45 | 45 | 45 | 42 |
| AFP | 41 | 32 | 45 | 43 |
| NSW CC | 44 | 44 | 45 | 45 |
| NSW Police | 36 | 24 | - | - |
| SA Police | 44 | 32 | 44 | 32 |
| **Average** | **42** | **35** | **45** | **41** |

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
- 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 | |
|---|---|---|---|---|---|---|
| | 12/13 | 13/14 | 12/13 | 13/14 | 12/13 | 13/14 |
| ACC[17] | 9 | 9 | 9 | 9 | 8 | 1 |
| ACLEI | - | - | - | 1 | 1 | 3 |
| AFP | 22 | 64 | 4 | 2 | 28 | 23 |
| CCC (QLD) | 1 | - | 1 | - | - | 2 |
| ICAC (NSW) | 1 | 1 | - | 2 | - | 2 |
| NSW CC | 5 | 12 | 19 | 27 | 24 | 15 |
| NSW Police | 72 | 79 | 25 | 48 | 14 | 34 |
| PIC | - | 4 | 28 | - | - | 3 |
| QLD Police | 14 | 14 | 12 | 4 | 1 | 3 |
| SA Police | 2 | 6 | - | - | - | 1 |
| TAS Police | - | 5 | - | - | - | - |
| NT Police | - | - | - | 1 | - | - |
| CCC (WA) | - | 6 | - | 1 | - | 2 |
| VIC Police | 8 | 2 | - | - | - | - |
| WA Police | 9 | - | 17 | 30 | 1 | 1 |
| **Total** | **143** | **202** | **115** | **125** | **77** | **90** |

## 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.

17 The ACC has provided revised figures for the 2012–13 reporting period. Table 13 provides these new figures.

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

| Agency | Total number of warrants | Number of eligible warrants | % |
|---|---|---|---|
| ACC | 192 | 124 | 65 |
| ACLEI | 32 | 8 | 25 |
| AFP | 458 | 245 | 53 |
| CCC (WA) | 66 | 37 | 56 |
| CCC (QLD) | 42 | 15 | 36 |
| ICAC (NSW) | 21 | 7 | 33 |
| NSW CC | 411 | 366 | 89 |
| NSW Police | 1,579 | 1,222 | 77 |
| NT Police | 50 | 22 | 44 |
| PIC | 35 | 13 | 37 |
| QLD Police | 337 | 322 | 96 |
| SA Police | 132 | 87 | 66 |
| TAS Police | 34 | 24 | 71 |
| VIC Police | 205 | 150 | 73 |
| IBAC | 16 | 10 | 63 |
| ICAC (SA) | 6 | 3 | 50 |
| WA Police | 339 | 191 | 56 |
| **TOTAL** | **3,955** | **2,846** | **72** |

## 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. There were no interceptions under subsection 7(4) of the TIA Act in 2011–12 and 2012–13.

**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 | |
| | 12/13 | 13/14 | 12/13 | 13/14 | 12/13 | 13/14 | 12/13 | 13/14 |
| AFP | - | - | 1 | 5 | - | - | - | - |
| **Total** | **-** | **-** | **1** | **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 | |
| | 12/13 | 13/14 | 12/13 | 13/14 | 12/13 | 13/14 | 12/13 | 13/14 |
| AFP | - | - | - | 5 | - | - | - | - |
| NSW Police | - | - | - | - | - | - | - | 1 |
| **Total** | **-** | **-** | **-** | **5** | **-** | **-** | **-** | **1** |

## 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 paragraph 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*. Consistent with the 2012–13 reporting period, agencies reported that no information was provided under these provisions in 2013–14.

## 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 | ACLEI | 10 |
| ACC | CCC (QLD) | 49 |
| AFP | ACLEI | 40 |
| NSW Police | NSW CC | 1 |
| VIC Police | TAS Police | 40 |
| IBAC | ICAC (SA) | 3 |
| **Total** | | **143** |

## 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 less warrants.

**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)**

| Agency | Total expenditure ($) | Average expenditure ($) |
|---|---|---|
| ACC | 7,210,000 | 28,498 |
| ACLEI | 787,497 | 31,500 |
| AFP | 10,541,869 | 15,412 |
| CCC (WA) | 1,431,412 | 22,366 |
| CCC (QLD) | 1,493,116 | 39,293 |
| IBAC | 1,454,405 | 90,900 |
| ICAC (NSW) | 252,289 | 12,014 |
| NSW CC | 3,072,249 | 8,803 |
| NSW Police | 6,805,841 | 4,495 |
| NT Police | 925,139 | 21,515 |
| PIC | 1,498,153 | 42,804 |
| QLD Police | 4,741,294 | 15,596 |
| ICAC (SA) | 45,420 | 7,570 |
| SA Police | 2,961,807 | 22,438 |
| TAS Police | 557,000 | 15,914 |
| VIC Police | 6,670,207 | 35,480 |
| WA Police | 3,467,883 | 11,560 |

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[18] | 5,877,274 | 158,635 | 192,224 | 980,807 | **7,208,940** |
| ACLEI | 611,203 | 140,820 | - | 35,473 | **787,496** |
| AFP | 8,103,605 | 174,597 | 1,760,955 | 502,712 | **10,541,869** |
| CCC (WA) | 1,046,391 | 7,906 | 296,853 | 80,262 | **1,431,412** |
| CCC (QLD) | 928,879 | 132,054 | - | 432,182 | **1,493,115** |
| ICAC (NSW) | 194,563 | - | - | 57,726 | **252,289** |
| NSW CC | 2,033,475 | - | 345,056 | 693,718 | **3,072,249** |
| NSW Police | 5,252,529 | 118,379 | - | 1,434,933 | **6,805,841** |
| NT Police | 672,126 | - | 123,459 | 129,554 | **925,139** |
| PIC | 1,248,038 | - | - | 250,115 | **1,498,153** |
| QLD Police | 3,097,332 | 614,886 | 281,380 | 747,695 | **4,741,293** |
| SA Police | 2,302,870 | 261,661 | 198,581 | 198,695 | **2,961,807** |
| TAS Police | 400,000 | 50,000 | 60,000 | 47,000 | **557,000** |
| VIC Police | 5,370,790 | 241,491 | 59,048 | 998,878 | **6,670,207** |
| IBAC | 1,122,373 | 54,962 | 93,200 | 183,870 | **1,454,405** |
| ICAC (SA) | 3,840 | - | 17,280 | 24,300 | **45,420** |
| WA Police | 3,099,492 | 204,757 | - | 163,634 | **3,467,883** |

## 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.

18 The ACC has advised the Attorney-General's Department that the 2012–13 recurrent cost should be revised up from a total amount of $6,586,933 to $6,640,761.

**Table 22: Emergency service facility declarations**

| State/territory | Police | Fire brigade | Ambulance | Emergency services authority | Despatching |
|---|---|---|---|---|---|
| New South Wales | 8 | 97 | 7 | - | 4 |
| Victoria | 18 | - | 30 | 3 | 22 |
| Queensland | 21 | 12 | 6 | - | 12 |
| Western Australia | 1 | 2 | 2 | 2 | 4 |
| South Australia | 3 | 2 | 1 | - | 3 |
| Tasmania | 1 | 2 | 1 | - | 2 |
| Australian Capital Territory | 3 | - | - | - | 3 |
| Northern Territory | 2 | - | 1 | 1 | 4 |
| **Total** | **57** | **115** | **48** | **6** | **54** |

## 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 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).

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

Overall, the Ombudsman considered that agencies demonstrated a good understanding of the Act's requirements, with all agencies found to be compliant with the majority of the Ombudsman's inspection criteria. The Ombudsman's inspection criteria (see Figures 4 and 5) are:

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

## Commonwealth Ombudsman's summary of findings

**Table 23: Summary of findings from the two inspections conducted at each agency during the reporting period**

| Criteria | ACC | ACLEI | AFP |
|---|---|---|---|
| Ss7 and 63 – Interceptions conducted in accordance with warrant, any unlawful information properly dealt with | Nothing to indicate otherwise | Nothing to indicate otherwise, with one exception[19] | Nothing to indicate otherwise |
| S49 – Warrants in the correct form | Compliant except for issues noted[20] | Compliant, except for issue noted[21] | Compliant except for issues noted[22] |
| S79 – Restricted records properly destroyed | Compliant | Not assessed as no records destroyed | Not assessed as no records destroyed |
| S80 – Requisite records kept in connection with issue of warrant | Compliant, except for issue noted[23] | Compliant | Compliant, except for issue noted[24] |
| S81 – Requisite records kept in connection with interceptions | Compliant | Compliant | Compliant, except for issue noted[25] |

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

## Commonwealth Ombudsman's findings for individual agency

### ACC

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

The Ombudsman acknowledged the commitment of the ACC to ensuring and improving agency compliance with TIA Act. In April 2014, the ACC introduced a compulsory online e-Learning module that staff will be required to undertake prior to being able to apply the provisions of the TIA Act.

19 Intercepted information from one warrant was not quarantined after ACLEI identified that the telecommunications number was no longer being used by the person listed on the warrant. ACLEI advised the Ombudsman it has taken measures to address this.

20 Two warrants had minor errors. The ACC self-disclosed that one warrant was not issued for a serious offence as it was not an ACC special investigation, one warrant referred to serious offences not listed in the affidavit and two warrants stated incorrect expiry dates. All self-disclosed warrants were voluntarily revoked.

21 Four warrants referred to 'issuing authority' rather than eligible Judge or nominated AAT member.

22 In eight instances, one self-disclosed and voluntarily revoked, warrants were not in the prescribed form. The AFP has advised the Ombudsman that training is ongoing. The AFP self-disclosed that two warrants were issued for longer than 90 days and one warrant was issued without an issue date. These warrants were voluntarily revoked.

23 A new warrant was given the same warrant number as the warrant it replaced. The ACC subsequently informed the Attorney-General's Department about the additional warrant.

24 In one instance, only a certified copy of the warrant was kept on file.

25 In one instance, the particulars relating to the use of legally intercepted information were not kept.

## ACLEI

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

The Ombudsman noted in relation to one warrant that interception continued ten days after the carrier subscribed the telecommunications number to a different person (it appears the carrier did not advise ACLEI of the change). Initially, intercepted information not associated with the target was not quarantined and was still available to investigators. The Ombudsman reported that ACLEI advised that the information was not provided to investigators or used during ACLEI hearings and following the Ombudsman's inspection was quarantined. ACLEI advised the Ombudsman that it has since addressed this issue.

## AFP

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

The Ombudsman noted several instances where warrants were not in the prescribed form. The Ombudsman reported that in conjunction with ongoing training, the AFP was reviewing the prescribed forms to ensure key areas to be completed in the form were clear.

## 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)).

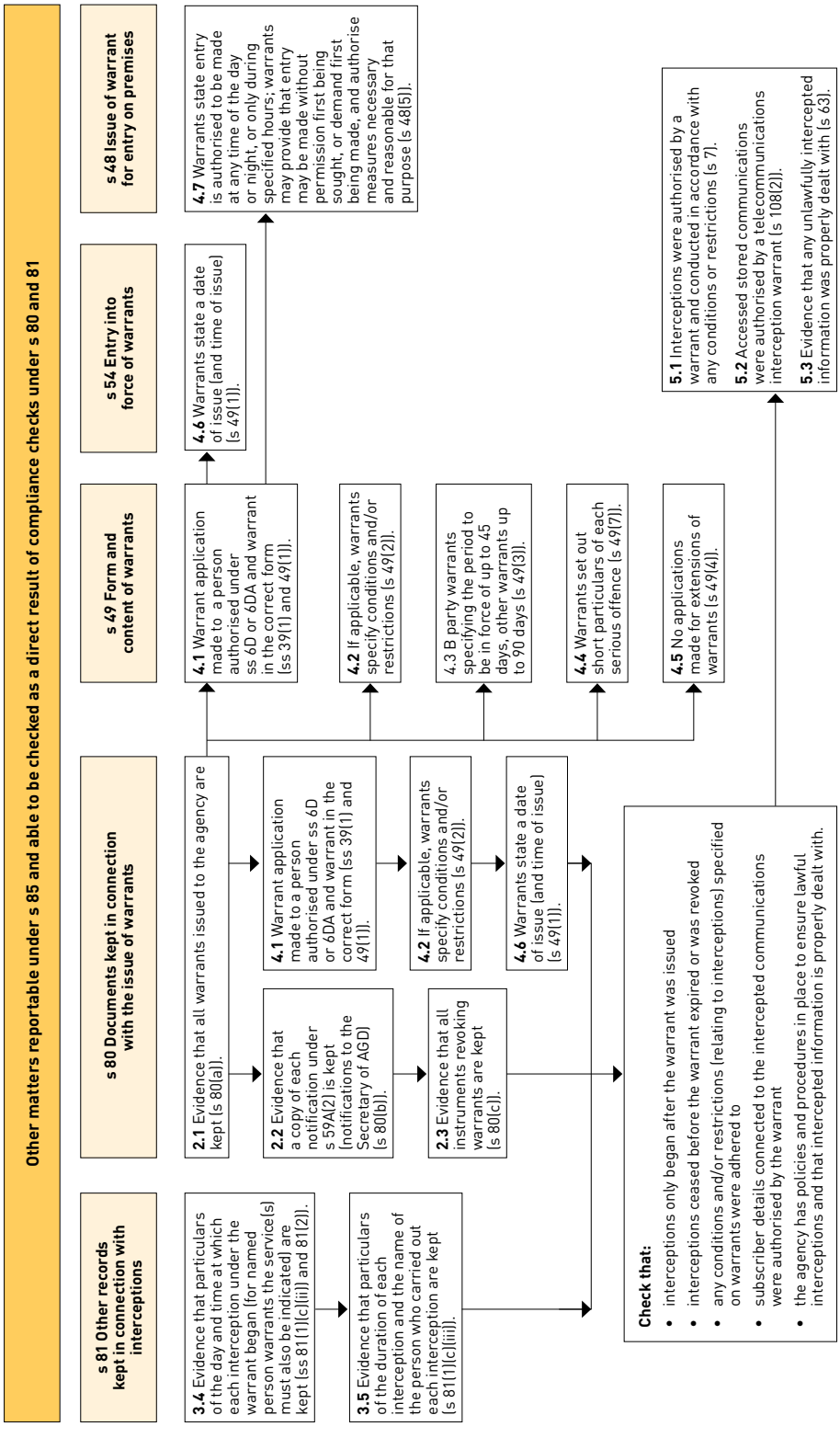
**3.10** Evidence that particulars of each other agency from or to which or other person from or to whom the agency received or supplied the restricted record are kept (s 81(1)(d)(iv)).

**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. In 2013–14, stored communications warrants were issued to several interception agencies and ASIC and Customs.

**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 | |
|---|---|---|---|---|---|
| | | 12/13 | 13/14 | 12/13 | 13/14 |
| ACC | Made | 10 | 4 | - | - |
| | Refused/withdrawn | - | - | - | - |
| | Issued | 10 | 4 | - | - |
| ICAC (NSW) | Made | - | 3 | - | - |
| | Refused/withdrawn | - | - | - | - |
| | Issued | - | 3 | - | - |
| AFP | Made | 44 | 39 | - | - |
| | Refused/withdrawn | - | - | - | - |
| | Issued | 44 | 39 | - | - |
| ASIC | Made | - | 3 | - | - |
| | Refused/withdrawn | - | - | - | - |
| | Issued | - | 3 | - | - |
| CCC (WA) | Made | - | 1 | - | - |
| | Refused/withdrawn | - | - | - | - |
| | Issued | - | 1 | - | - |
| CCC (QLD) | Made | 1 | 1 | - | - |
| | Refused/withdrawn | - | - | - | - |
| | Issued | 1 | 1 | - | - |
| CUSTOMS | Made | 8 | 12 | - | - |
| | Refused/withdrawn | - | - | - | - |
| | Issued | 8 | 12 | - | - |
| NSW CC | Made | 3 | 8 | - | - |
| | Refused/withdrawn | - | - | - | - |
| | Issued | 3 | 8 | - | - |
| NSW Police | Made | 233 | 233 | - | 1 |
| | Refused/withdrawn | - | - | - | - |
| | Issued | 233 | 233 | - | 1 |
| NT Police | Made | 15 | 5 | - | - |
| | Refused/withdrawn | - | - | - | - |
| | Issued | 15 | 5 | - | - |
| PIC | Made | 4 | 4 | - | - |
| | Refused/withdrawn | - | - | - | - |
| | Issued | 4 | 4 | - | - |
| QLD Police | Made | 101 | 107 | - | - |
| | Refused/withdrawn | - | 1 | - | - |
| | Issued | 101 | 106 | - | - |
| SA Police | Made | 11 | 21 | - | - |
| | Refused/withdrawn | - | - | - | - |
| | Issued | 11 | 21 | - | - |

| Agency | Relevant statistics | Applications for stored communications warrants | | Telephone applications for stored communications warrants | |
|---|---|---|---|---|---|
| | | 12/13 | 13/14 | 12/13 | 13/14 |
| TAS Police | Made | 47 | 52 | - | - |
| | Refused/withdrawn | - | - | - | - |
| | Issued | 47 | 52 | - | - |
| VIC Police | Made | 26 | 47 | - | - |
| | Refused/withdrawn | - | - | - | - |
| | Issued | 26 | 47 | - | - |
| WA Police | Made | 59 | 32 | 1 | - |
| | Refused/withdrawn | 1 | - | - | - |
| | Issued | 58 | 32 | 1 | - |
| **Total** | **Made** | **562** | **572** | **1** | **1** |
| | **Refused/withdrawn** | **1** | **1** | **-** | **-** |
| | **Issued** | **561** | **571** | **1** | **1** |

## Effectiveness of stored communications warrants

In 2013–14 law enforcement agencies made 153 arrests, conducted 176 proceedings and obtained 144 convictions based on evidence obtained under stored communications warrants.

**Table 25: Number of arrests, proceedings and convictions made on the basis of lawfully accessed information—s. 163(a)-(b)**

| Agency | Arrests | | Proceedings | | Convictions | |
|---|---|---|---|---|---|---|
| | 12/13 | 13/14 | 12/13 | 13/14 | 12/13 | 13/14 |
| ACC | 1 | 15 | - | 8 | - | - |
| AFP | 18 | 23 | 12 | 19 | 3 | 1 |
| ASIC | - | - | - | - | 3 | - |
| CCC (WA) | - | - | - | 2 | - | 2 |
| CUSTOMS | - | 4 | - | 1 | - | 1 |
| NSW Police | 56 | 51 | 123 | 138 | 46 | 121 |
| NT Police | 6 | 2 | - | - | - | - |
| QLD Police | 18 | 23 | 4 | - | 4 | - |
| TAS Police | 15 | 1 | 6 | 1 | 5 | 1 |
| VIC Police | 10 | 21 | 5 | 3 | 4 | 16 |
| WA Police | 8 | 13 | 2 | 4 | - | 2 |
| **Total** | **132** | **153** | **152** | **176** | **65** | **144** |

In 2012–13 law enforcement agencies made 132 arrests, conducted 152 prosecutions and obtained 65 convictions based on evidence obtained under stored communications warrants.

Care should be taken in interpreting Table 25 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 lapsed 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 2013–14, 1,511 domestic preservation notices and 467 domestic preservation revocation notices were issued (see Table 26).

The Ombudsman has functions in relation to preservation notices given by issuing agencies (other than the Organisation) and the InspectorGeneral of Intelligence and Security has functions in relation to preservation notices given by the Organisation.

**Table 26: Domestic preservation notices—s. 161A(1)**

| Agency | Domestic preservation notice issued | Domestic preservation notice revocations issued |
|---|---|---|
| ACC | 40 | 2 |
| AFP | 170 | 79 |
| ASIC | 143 | 4 |
| CCC (WA) | 1 | - |
| CCC (QLD) | 33 | 7 |
| NSW ICAC | 8 | - |
| NSW CC | 7 | 1 |
| NSW Police | 318 | 55 |
| NT Police | 36 | 16 |
| PIC | 8 | - |
| QLD Police | 353 | 136 |
| SA Police | 64 | 43 |
| TAS Police | 133 | 85 |
| VIC Police | 75 | 11 |
| CUSTOMS | 23 | 1 |
| ACLEI | 9 | 4 |
| WA Police | 90 | 23 |
| **Total** | **1,511** | **467** |

Under section 161A(2) of the TIA Act the AFP is required to report on foreign preservation notices. In 2013–14, the AFP reported that six foreign preservation notices and no foreign preservation notice revocation notices were issued.

## Mutual assistance

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

**Table 27: Mutual assistance and stored communications warrants—s. 162(1)(c)**

| Agency | Number of stored communications warrants applied for as a result of mutual assistance | | Number of stored communications warrants refused | | Number of stored communications warrants issued as a result of mutual assistance | |
|---|---|---|---|---|---|---|
| | 12/13 | 13/14 | 12/13 | 13/14 | 12/13 | 13/14 |
| AFP | 6 | - | - | - | 6 | - |
| **Total** | **6** | **-** | **-** | **-** | **6** | **-** |

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 2013–14 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 access records

During the reporting period the Commonwealth Ombudsman inspected the preservation notices and stored communications access records of 17 enforcement agencies. The inspections are on the basis of a full year, and for this reason, the Ombudsman's inspections of the enforcement agencies related to 2012–13 records.

During the 2013–14 inspection period, the Ombudsman noted that agencies have implemented the Ombudsman's previous suggestions and recommendations, updating relevant policies and procedures to help staff to comply with the TIA Act. The Ombudsman's inspection criteria are:

1. Were destructions properly conducted (sections 150 and 151(e))?
2. Were records properly kept (sections 150A and 151)?
3. Were preservation notices properly given (sections 107H(2), 107H(3), 107M, 107N, and 107S)?
4. Were preservation notices properly revoked (sections 107L, 107M, 107R and 107S)?
5. Were warrant applications properly made and warrants in the correct form (sections 113, 5E, 6B, 116(1)(d), 116(1)(da), 6DB, 118, and 119(5))?
6. Were warrants properly revoked (sections 122 and 123)?
7. Were conditions and restrictions on warrants adhered to (section 117)?
8. Was the authority of the warrant only exercised by an authorised officer and was lawfully accessed information only communicated to authorised officers (sections 127(1) and (2), and 135(2))?
9. Were stored communications accessed in accordance with the Act (sections 108, 117 and 119) and were any unlawfully accessed stored communications properly dealt with (section 133)?

### Overall

During 2013–14, the Ombudsman noted that most agencies displayed a positive attitude towards compliance and had adopted the Ombudsman's suggestions from 2012–13. In particular, the Ombudsman noted that agencies have implemented measures to assure themselves that they are only dealing with lawfully accessed stored communications provided by carriers.

During this period the Ombudsman also conducted his first inspections of agencies' preservation notice records.

## Record keeping compliance

Most agencies were assessed as compliant with the record keeping requirements relating to preservation notices and stored communications warrants under sections 150A and 151 of the TIA Act; however the Ombudsman made a small number of formal recommendations to agencies that they improve their record keeping procedures. The Ombudsman reported that agencies were generally responsive to these recommendations.

## Preservation notices

The Ombudsman identified a number of instances where preservation notices were not given and revoked in accordance with the TIA Act. As a result, the Ombudsman made a number of suggestions to agencies that they improve their processes to improve compliance with the TIA Act. The Ombudsman reported that agencies were generally responsive to these suggestions.

## Destructions

The Ombudsman reported that most agencies destroyed records under section 150 of the TIA Act, but that a number of these agencies were assessed as not compliant with certain provisions under section 150. Issues arose from reports not being submitted to the Attorney-General or destructions not occurring in accordance with the TIA Act. In some of these instances, the Ombudsman noted that agencies had destroyed the information for purposes such as limiting the use and disclosure of accessed stored communications.

## Applying for warrants

Based on the records made available at four of the inspected agencies, the Ombudsman identified deficiencies in the information provided to issuing authorities. Some agencies agreed with the Ombudsman's findings and in response advised of appropriate actions while others advised that they were satisfied that sufficient information was provided.

## Dealing with accessed stored communications provided by carriers

During 2013–14, the Ombudsman again identified a number of instances where it appeared that stored communications that were not sent to or by the person named on the warrant were accessed by carriers and provided to several agencies, and where carriers had accessed stored communications after the relevant warrant had already expired. The Ombudsman reiterated to agencies the importance of "screening" all stored communications they receive from carriers to ensure that they are only dealing with lawfully accessed information.

**Figure 6: Commonwealth Ombudsman—stored communications access inspection criteria**

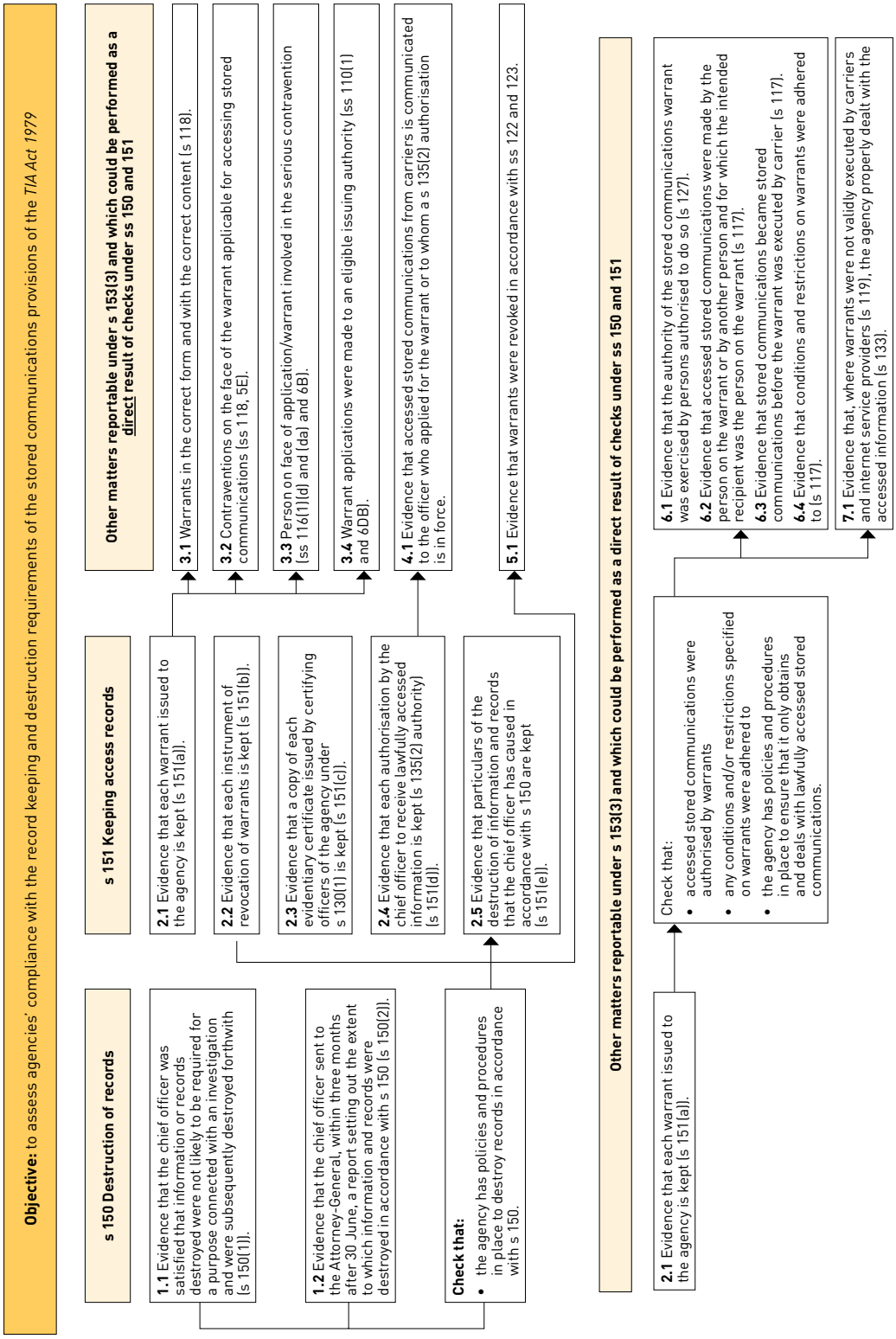
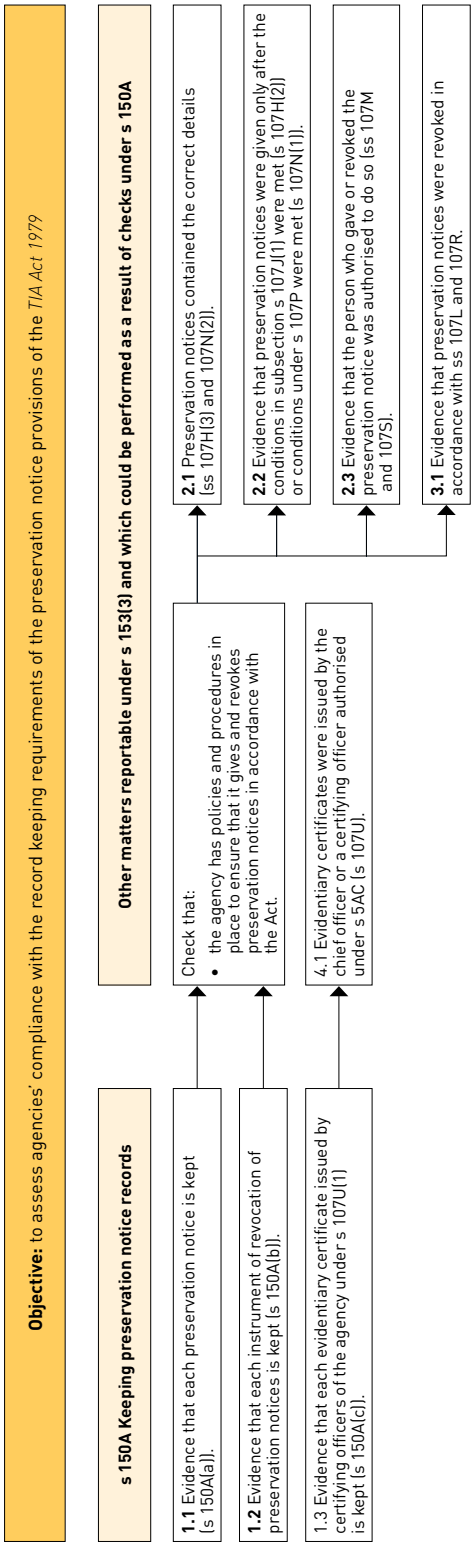


**Figure 7: Commonwealth Ombudsman—preservation notice inspection criteria**



# 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 2013–14, 77 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.

## 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.

**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 | |
|---|---|---|
| | 12/13 | 13/14 |
| ACC | 3,789 | 5,447 |
| ACLEI | 2,594 | 2,244 |
| AFP | 25,582 | 21,358 |
| CCC (WA) | 1,538 | 1,804 |
| CCC (QLD) | 7,646 | 10,896 |
| IBAC | 20 | 321 |
| ICAC (NSW) | 575 | 933 |
| NSW CC | 3,120 | 3,294 |
| NSW Police | 119,705 | 111,889 |
| NT Police | 3,308 | 10,182 |
| OPI | 71 | - |
| PIC | 1,771 | 1,475 |
| QLD Police | 41,120 | 35,663 |
| SA Police | 9,119 | 8,504 |
| TAS Police | 8,701 | 9,921 |
| VIC Police | 64,458 | 63,325 |
| ICAC (SA) | - | 16 |
| WA Police | 19,812 | 27,315 |
| **Total** | **312,929** | **314,587** |

In 2013–14, enforcement agencies made 324,260 data authorisations to enforce the criminal law. This was an increase of 4,228 or 1.3 per cent from the previous reporting period.

CASE STUDY:
## AUSTRALIAN FEDERAL POLICE

Telecommunications data has played a pivotal role in bringing to justice an individual involved with child exploitation.

In February 2014, the Australian Federal Police received information regarding a person suspected of uploading suspicious photographs to an image-sharing website. Two different IP addresses were used by the suspect and requests were submitted to the relevant telecommunications companies to identify the users of the IPs. Data was not available for one of the IP addresses; however, data relating to the second IP address identified a subscriber and a location. The subscriber details provided by the telecommunications company gave police sufficient information to obtain search warrants, which led to the discovery of a large volume of child pornography material and information indicating possible abuse. The individual in possession of the material was subsequently arrested.

CASE STUDY:
## VICTORIA POLICE

Telecommunications data has provided Victoria Police with the information to bring about the successful arrest and prosecution of individuals involved in a series of previously unsolved crimes.

VICTORIA POLICE

In 2012, a person was the target of sustained racially motivated violence which included the fire-bombing of the victim's business on two occasions. Although the victim was able to suggest a suspect police did not have enough evidence to arrest that person. CCTV footage of both fire bombings identified the vehicle used by the offender/s. The same vehicle was found burnt out the day after the owner had reported to police that the vehicle had been stolen. The crimes remained unsolved and were handed to an investigation team for review during the first half of 2013.

The investigation team accessed the telecommunications data of the owner of the stolen vehicle and analysis of this data revealed that the owner of the stolen car had been in contact with the arson suspect during the time his car was stolen, and during the times the arson was committed. The data also contradicted the statement the vehicle's owner had made to police about the theft of his vehicle.

Close analysis of the CCTV footage showed that as the offender was in the process of lighting the fire, his mobile phone rang in his pocket, causing him to turn it off. The time on the CCTV footage and the time of the phone call (based on the telecommunications data received) showed that the owner of the vehicle

made a hangup call to the offender at the exact moment the offender grabbed his phone and turned it off. Further to this, the call charge records showed that this crucial call passed through a cell tower located only 50 to 100 metres from the victim's business.

The call charge records were used to identify two further suspects from both arsons, and exculpated suspects from other violent offences the victim had suffered. Information provided by these records resulted in the identified offenders being charged with arson and associated offences, and both subsequently pleaded guilty to the charges.

**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 | |
|---|---|---|
| | 12/13 | 13/14 |
| ACCC | 134 | 10 |
| Australian Fisheries Management Authority | 2 | 3 |
| ASIC | 1,336 | 1,771 |
| Australian Taxation Office | 493 | 277 |
| Civil Aviation Safety Authority | 4 | - |
| Customs | 3,902 | 6,196 |
| Dept. of Agriculture | 84 | 84 |
| Dept. of Defence | 14 | 25 |
| Dept. of Families, Housing, Community Services and Indigenous Affairs | 4 | - |
| Dept. of Foreign Affairs and Trade | 84 | - |
| Dept. of Health | 76 | 38 |
| Dept. of Human Services | 1 | - |
| Dept. of Immigration and Border Protection[26] | 158 | 107 |
| Dept. of Social Services | - | 1 |
| Dept. of the Environment | 9 | 13 |
| Australian Financial Security Authority | 111 | 128 |
| **Total** | **6,412** | **8,653** |

26 The 2012–13 figures have been revised to include information about the Department of Immigration and Border Protection. This information was not included in the original report.

**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 | |
|---|---|---|
| | 12/13 | 13/14 |
| Bankstown City Council | 5 | - |
| Corrective Services NSW | 69 | 52 |
| Corrections Victoria | - | 389 |
| Dept. of Commerce (WA) | 116 | 78 |
| Dept. of Environment and Primary Industries (VIC) | 349 | 347 |
| Office of Environment & Heritage (NSW) | 106 | 47 |
| RSPCA Queensland | 8 | - |
| RSPCA Victoria | 23 | 64 |
| Transport Accident Commission (VIC) | 1 | 8 |
| NSW Environment Protection Authority | - | 5 |
| Workcover NSW | - | 4 |
| The Hills Shire Council | - | 1 |
| Victorian Workcover Authority | 14 | 25 |
| **Total** | **691** | **1,020** |

**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 | |
|---|---|---|
| | 12/13 | 13/14 |
| No. of authorisations made by a Law Enforcement Agency | 312,929 | 314,587 |
| No. of authorisations made by a Commonwealth Agency[27] | 6,412 | 8,653 |
| No. of authorisations made by a State or Territory Agency | 691 | 1,020 |
| **Total** | **320,032** | **324,260** |

## 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.

27 This figure has been revised to include information from the Department of Immigration and Border Protection.

In 2013–14, enforcement agencies made 10,398 data authorisations to enforce a law that imposes a pecuniary penalty or protects the public revenue. This was a decrease of 368 authorisations or 3.4 per cent from the previous reporting period.

**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 | |
|---|---|---|
| | 12/13 | 13/14 |
| AFP | 99 | 36 |
| NSW Police | 6,300 | 5,324 |
| NT Police | 2 | 4 |
| QLD Police | 110 | 239 |
| SA Police | - | 2 |
| CCC (QLD) | - | 11 |
| TAS Police | 67 | 764 |
| **Total** | **6,578** | **6,380** |

**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 | |
|---|---|---|
| | 12/13 | 13/14 |
| ACCC | 155 | 31 |
| Australian Health Practitioner Regulation Agency | 20 | 23 |
| ASIC | 114 | 110 |
| Australian Taxation Office | 138 | 66 |
| Australia Post | 375 | 810 |
| Civil Aviation Safety Authority | 3 | - |
| Clean Energy Regulator | 1 | 1 |
| Customs | 120 | 156 |
| Dept. of Agriculture | 8 | - |
| Dept. of Defence | 127 | 94 |
| Dept. of Foreign Affairs and Trade | 67 | 227 |
| Dept. of Health | 1 | - |
| Dept. of Human Services | 628 | 339 |

| Agency | Authorisations | |
|---|---|---|
| | 12/13 | 13/14 |
| Dept. of Immigration and Border Protection | 14 | - |
| Dept. of Social Services | - | 1 |
| Fair Work Building & Construction | 1 | 7 |
| National Measurement Institute | - | 1 |
| Tax Practitioners Board | 61 | - |
| **Total** | **1,833** | **1,866** |

**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 | |
|---|---|---|
| | 12/13 | 13/14 |
| ACT Revenue Office | 6 | 3 |
| Bankstown City Council | 5 | 7 |
| City of Darebin | - | 1 |
| Consumer Affairs Victoria | 187 | 120 |
| Consumer and Business Services (SA) | 209 | 153 |
| Dept. of Agriculture, Fisheries and Forestry (QLD) | 33 | 25 |
| Dept. of Commerce (WA) | 84 | 87 |
| Dept of Environment and Heritage Protection (QLD) | 55 | 32 |
| Dept. of Environment & Primary Industries (VIC) | 51 | - |
| Dept. of Fisheries (WA) | 101 | 113 |
| Dept. of Justice (VIC) | - | 16 |
| Dept. of Mines And Petroleum (WA) | - | 2 |
| Dept. of Parks And Wildlife (WA) | 87 | 6 |
| Dept. of Primary Industries (NSW) | 197 | 226 |
| Harness Racing New South Wales | 12 | 7 |
| Harness Racing Victoria | - | 3 |
| Health Care Complaints Commission (NSW) | 15 | 20 |
| Ipswich City Council | 6 | 21 |
| Knox City Council | 5 | 5 |
| Legal Services Board (VIC) | - | 9 |

| Agency | Authorisations | |
|---|---|---|
| | 12/13 | 13/14 |
| NSW Fair Trading | 740 | 758 |
| Office of Fair Trading (QLD) | 257 | 252 |
| Office of Liquor and Gaming Regulation (QLD) | 2 | 3 |
| Office of State Revenue (NSW) | 137 | 127 |
| Office of State Revenue (QLD) | 5 | 1 |
| Office of the Racing Integrity Commissioner (VIC) | 15 | 10 |
| Racing and Wagering Western Australia | 10 | 18 |
| Racing NSW | 14 | 16 |
| Racing Queensland | 28 | 4 |
| Revenue SA | 18 | 17 |
| Roads and Maritime Services (NSW) | 4 | - |
| RSPCA South Australia | 1 | - |
| RSPCA Queensland | - | 19 |
| State Revenue Office Victoria | 40 | 53 |
| Tasmania Prison Service | 15 | - |
| Workcover NSW | 1 | - |
| Victorian Workcover Authority | - | 17 |
| Wyndham City Council | 15 | 1 |
| **Total** | **2,355** | **2,152** |

**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 | |
|---|---|---|
| | 12/13 | 13/14 |
| No. of authorisations made by a Law Enforcement Agency | 6,578 | 6,380 |
| No. of authorisations made by a Commonwealth Agency | 1,833 | 1,866 |
| No. of authorisations made by a State or Territory Agency | 2,355 | 2,152 |
| **Total** | **10,766** | **10,398** |

## Prospective data—authorisations

Tables 36 and 37 set out information about the use of prospective data authorisations during the reporting year.

**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 | 1,075 | 29,774 | 19,030 | 73 |
| AFP | 1,037 | 33,691 | 22,174 | 145 |
| IBAC | 189 | 8,420 | 5,601 | 38 |
| CCC (WA) | 47 | 1,613 | 1,136 | 1 |
| CCC (QLD) | 394 | 7,246 | 6,189 | 51 |
| CUSTOMS | 144 | 169 | 163 | 1 |
| ICAC (NSW) | 30 | 1,350 | 1,002 | 1 |
| NSW CC | 770 | 27,849 | 20,166 | 75 |
| NSW Police | 567 | 21,484 | 13,235 | 33 |
| NT Police | 334 | 15,030 | 14,534 | 13 |
| ACLEI | 8 | 66 | 21 | 7 |
| PIC | 146 | 5,885 | 4,741 | 15 |
| QLD Police | 3,857 | 163,233 | 127,006 | 414 |
| SA Police | 260 | 10,995 | 7,613 | 19 |
| TAS Police | 166 | 7,470 | 4,407 | 17 |
| VIC Police | 3,339 | 48,668 | 30,666 | 53 |
| WA Police | 752 | 33,840 | 24,429 | 79 |
| **Total** | **13,115** | **416,783** | **302,113** | **1,035** |

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 37.

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 38 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 | |
|---|---|---|---|---|
| | 12/13 | 13/14 | 12/13 | 13/14 |
| ACC | 35 | 28 | 24 | 19 |
| ACLEI | - | 8 | - | 21 |
| AFP | 32 | 32 | 27 | 25 |
| CCC (WA) | 41 | 34 | 35 | 25 |
| CCC (QLD) | 24 | 18 | 20 | 18 |
| CUSTOMS | 1 | 1 | 1 | 1 |
| IBAC | 44 | 45 | - | 37 |
| ICAC (NSW) | 44 | 45 | 33 | 35 |
| NSW CC | 36 | 36 | 32 | 29 |
| NSW Police | 38 | 38 | 25 | 25 |
| NT Police | 45 | 45 | 42 | 45 |
| OPI | 44 | - | 44 | - |
| PIC | 41 | 40 | 37 | 36 |
| QLD Police | 39 | 42 | 32 | 37 |
| SA Police | 41 | 42 | 36 | 32 |
| TAS Police | 45 | 45 | 29 | 30 |
| VIC Police | 39 | 15 | 28 | 9 |
| WA Police | 45 | 45 | 30 | 36 |
| **Average** | **37** | **33** | **30** | **27** |

## 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 | |
|---|---|---|
| | 12/13 | 13/14 |
| AFP | 45 | 55 |
| NSW Police | 570 | 1,097 |
| NT Police | 17 | 36 |
| SA Police | - | 33 |
| TAS Police | - | 155 |
| QLD Police | 263 | 652 |
| **Total** | **895** | **2,028** |

## 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 2013–14, the AFP made 19 data authorisations for access to historical information to enforce the criminal law of a foreign country.

Following these requests, the AFP made 17 disclosures to foreign law enforcement agencies. Information was disclosed to the following countries: France, Germany, Greece, Hong Kong (The Special Administrative Region of the People's Republic of China), Hungary, India, Italy, Japan, Lithuania, Norway, Poland, Russia, Sri Lanka and Singapore.

# 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


| | | |
|---|---|---|
| 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) | 6 |
| 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) | 7 |
| 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) | 8 |
| Table 4 | Applications for telecommunications interception warrants, telephone interception warrants and renewal applications—ss. 100(1)(a)-(c) and 100(2)(a)-(c) | 9 |
| Table 5 | Applications for telecommunications interception warrants authorising entry on premises—ss. 100(1)(d) and 100(2)(d) | 11 |
| Table 6 | Arrests on the basis of lawfully intercepted information—ss. 102(1)(a) and 102(2)(a) | 12 |
| Table 7 | Prosecutions in which lawfully intercepted information was given in evidence | 14 |
| Table 8 | Convictions in which lawfully intercepted information was given in evidence | 15 |
| 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) | 16 |
| Table 10 | Number of services intercepted under named person warrants—ss. 100(1)(eb) and 100(2)(eb) | 18 |
| Table 11 | Total number of services and devices intercepted under device-based named person warrants—ss. 100(1)(ec) and 100(2)(ec) | 19 |
| Table 12 | Applications for B-Party warrants, telephone applications for B-Party warrants, and renewal applications—ss. 100(1)(ed) and 100(2)(ed) | 20 |
| Table 13 | B-Party warrants issued with conditions or restrictions—ss. 100(1)(ed) and 100(2)(ed) | 21 |

| | | |
|---|---|---|
| Table 14 | Duration of original and renewal telecommunications interception warrants—ss. 101(1)(a)-(d) and 101(2)(a)-(d) | 22 |
| Table 15 | Duration of original and renewal B-Party warrants—ss. 101(1)(da) and 101(2)(da) | 23 |
| Table 16 | Number of final renewals—ss. 101(1)(e) and 101(2)(e) | 24 |
| Table 17 | Percentage of eligible warrants—ss. 102(3) and 102(4) | 25 |
| Table 18a | Interception without a warrant—s. 102A | 26 |
| Table 18b | Interception without a warrant—s. 102A | 26 |
| Table 19 | Number of interceptions carried out on behalf of other agencies—s. 103(ac) | 27 |
| 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) | 27 |
| Table 21 | Recurrent costs of interceptions per agency | 28 |
| Table 22 | Emergency service facility declarations | 29 |
| Table 23 | Summary of findings from the two inspections conducted at each agency during the reporting period | 31 |
| Table 24 | Applications and telephone applications for stored communications warrants—ss. 162(1)(a)-(b) and 162(2)(a)-(b) | 36 |
| Table 25 | Number of arrests, proceedings and convictions made on the basis of lawfully accessed information—s. 163(a)-(b) | 37 |
| Table 26 | Domestic preservation notices—s. 161A(1) | 39 |
| Table 27 | Mutual assistance and stored communications warrants—s. 162(1)(c) | 39 |
| 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) | 45 |
| 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) | 47 |
| 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) | 48 |
| 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) | 48 |
| 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) | 49 |

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) 49

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) 50

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) 51

Table 36 Prospective data authorisations—s. 186(1)(c) 52

Table 37: Average specified and actual time in force of prospective data authorisations 53

Table 38 The number of authorisations made for access to existing information or documents for the location of missing persons—s. 178A 54

## Figures

Figure 1 Telecommunications interception warrants issued with specific conditions or restrictions—ss. 100(1)(e) and 100(2)(e) 11

Figure 2 Named person warrants issued with conditions or restrictions—ss. 100(1)(ea) and 100(2)(ea) 18

Figure 3 Total number of services intercepted under service-based name person warrants—ss. 100(1)(ec) and 100(2)(ec) 19

Figure 4 Commonwealth Ombudsman's Telecommunications Interception Inspection Criteria 33

Figure 5 Other matters reportable under s.85 34

Figure 6 Commonwealth Ombudsman—stored communications access inspection criteria 42

Figure 7 Commonwealth Ombudsman—preservation notice inspection criteria 43

# 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

| | |
|---|---|
| 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 |
| IBAC | 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) |
| 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 |