Australian Government
Attorney-General's Department

# TELECOMMUNICATIONS (INTERCEPTION AND ACCESS) ACT 1979

## Annual Report 2015–16

ISBN 978-1-925290-48-6 (Print)

ISBN 978-1-925290-49-3 (Online)



**Contact us**

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

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

Email: copyright@ag.gov.au

# TELECOMMUNICATIONS (INTERCEPTION AND ACCESS) ACT 1979

**Annual Report 2015–16**

# CONTENTS

# EXECUTIVE SUMMARY

The *Telecommunications (Interception and Access) 1979 Act Annual Report 2015–16* sets out the extent and circumstances in which eligible Commonwealth, State and Territory government agencies have used the powers available under the *Telecommunications (Interception and Access) Act 1979* (TIA Act) between 1 July 2015—30 June 2016.

The primary function of the TIA Act is to allow lawful access to communications and data for law enforcement and national security purposes, in a way that protects the privacy of people who use the Australian telecommunications network. Serious and organised criminals and persons seeking to harm Australia's national security routinely use telecommunications services and communications technology to plan and carry out their activities.

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

The use of warrants to intercept and access stored communications is independently overseen by the Commonwealth Ombudsman and equivalent state bodies. The independent oversight role of the Commonwealth Ombudsman was extended to access and use of telecommunications data under the TIA Act on 13 October 2015.

## Legislative reforms

### Data Retention Act

The *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Data Retention Act) came into effect on 13 October 2015. The Data Retention Act standardised the data telecommunications companies are required to retain and introduced a mandatory retention period of two years. It also introduced a requirement for carriers to encrypt and protect retained data.

The Data Retention Act significantly limited the range of agencies that can apply for a warrant to access stored communications or authorise the disclosure of telecommunications data under the TIA Act. The ability to apply for a stored communications warrant is limited to 20 designated 'criminal law-enforcement agencies'. The ability for enforcement agencies to authorise the disclosure of telecommunications data has also been limited to the same 20 criminal law-enforcement agencies and the Australian Security Intelligence Organisation (ASIO).

The Data Retention Act also introduced additional record-keeping and reporting obligations relating to the access to and use of telecommunications data. This information is set out in Chapter 3 of this report.

### Public interest advocate regulations

The Data Retention Act prohibits ASIO and enforcement agencies from authorising the disclosure of telecommunications data of a journalist or their employer where a purpose of making the authorisation is to identify a journalist's source, unless a journalist information warrant has been obtained. The journalist information warrants regime recognises the public interest in protecting journalists' sources while ensuring agencies have the investigative tools necessary to protect the community.

When considering an application for a journalist information warrant, the TIA Act requires that the Attorney-General or issuing authority is satisfied that the public interest in issuing the warrant outweighs the public interest in protecting the confidentiality of the identity of the source. The regime is supported by the Public Interest Advocates who promote the rights of a journalist to seek and impart information by independently considering and evaluating warrant applications and providing independent submissions in the warrant application process. The *Telecommunications (Interception and Access) Regulations 1987* have been amended to set out the procedure for applying for a journalist information warrant. These Regulations support the role of Public Interest Advocates by ensuring effective consultation and allowing submissions to be made in warrant applications.

## Key judicial decisions

In 2015, a jury convicted three parties for offences under section 45 of the *Crimes Act 1900* (NSW), which prohibits female genital mutilation (FGM). The first party was convicted of performing FGM on two girls at the request of the second party, their mother. The third party was convicted as being an accessory after the fact in relation to the events. Electronic evidence gathered under the TIA Act and the *Surveillance Devices Act 2007* (NSW) formed a critical part of the police investigation, the prosecution case and the subsequent sentencing of the offenders. This was NSW's first successful prosecution for these types of offences and resulted in penalties ranging from home detention to imprisonment for 15 months.

## Key findings

- In 2015–16, 3,857 interception warrants were issued.
- During 2015–16, information obtained under interception warrants was used in:[1]
  - 3,019 arrests[2]
  - 3,726 prosecutions
  - 1,812 convictions.

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

2 This figure includes the number of times lawfully intercepted information culminated in an arrest.

- In 2015–16, 63 enforcement agencies made 333,980 authorisations for the disclosure of historical telecommunications data. Of these, 326,373 authorisations were made to enforce a criminal law. Due to the reduction in agencies authorised to request data, as a result of the Data Retention Act, 43 of these agencies only reported for the period between 1 July 2015 and 12 October 2015.
- From 13 October 2015—30 June 2016 the majority of criminal law offences for which historical data was requested was illicit drug offences (57,166 requests). 25,245 requests were made for homicide and related offences and 4,454 requests were made to assist in terrorism investigations.
- In 2015–16, 33 authorisations were made under two Journalist Information Warrants. This is the first year the Journalist Information Warrants scheme has been operating.
- In 2015–16, law enforcement agencies made 366 arrests, conducted 485 proceedings and obtained 195 convictions based on evidence obtained under stored communications warrants.[3]

## Access to the content of a communication

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

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

## Telecommunications data

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

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

---

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

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

Telecommunications data gives agencies a method for tracing telecommunications from end-to-end. It can also be used to demonstrate an association between people, or to prove that two or more people spoke with each other at a critical point in time.

Access to telecommunications data is regulated by Chapter 4 of the TIA Act, which permits an authority or body that is 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.

During the 2015–2016 reporting period all enforcement agencies could access historical data[5] and only criminal law-enforcement agencies could access prospective data to assist in the investigation of offences punishable by at least three years' imprisonment.[6] The Data Retention Act, passed by the Parliament in March 2015, reduced the number of enforcement agencies that may access telecommunications data to 20 specified agencies and ASIO. The Attorney-General may declare additional agencies in prescribed circumstances. No additional agencies were prescribed in the 2015–16 reporting period.

## Format of Annual Report

This Annual Report is organised into three main chapters:

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

The TIA Act and associated amendments are available online at <www.legislation.gov.au>

## More information

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

- Attorney-General's Department <www.ag.gov.au>
- Department of Communications and the Arts <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>

5 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.

6 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 under the circumstances set out in the TIA Act. For example, the prohibition against interception does not apply to communications intercepted through a warrant or in circumstances connected to the operation or maintenance of a telecommunications system.

**Definition**

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

The TIA Act provides for several types of warrants which enable access to real-time content (for example, a phone call while the parties are talking with each other). During the reporting period, interception warrants were available to 17 Commonwealth, state and territory agencies (along with ASIO) 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.[7]

Serious offences for which interception can be obtained under the TIA Act include murder, kidnapping, serious drug offences, terrorism, offences involving child pornography, money laundering, and offences involving organised crime.

The information provided in Table 1 illustrates the important role telecommunications interception plays in investigating serious crimes. Consistent with previous years, in 2015–16 the majority of warrants obtained were to assist with investigations into serious drug offences (2,178 warrants). Loss of life or personal injury offences were specified in 536 warrants and 439 warrants related to murder investigations. Money laundering was specified as an offence in 264 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 offences covered under each category is set out in Appendix D.

7 There are exceptions to this threshold. Interception warrants may be available for offences that typically involve the use of the telecommunications system, such as offences involving collusion. In these circumstances telecommunications interception is a critical investigative tool and its availability may be key to resolving an investigation.

**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 (QLD) | CCC (WA) | IBAC | ICAC (NSW) | ICAC (SA) | NSW CC | NSW Police | NT Police | PIC | QLD Police | SA Police | TAS Police | VIC Police | WA Police | TOTAL |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ACC special investigation | 260 | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | 260 |
| Administration of justice | - | - | 11 | - | - | - | - | - | - | - | - | - | - | - | - | - | - | 11 |
| Bribery, corruption and dishonesty offences | - | 9 | 42 | 11 | 25 | 4 | 12 | 8 | - | - | - | 42 | - | 5 | - | 3 | 9 | 170 |
| Cartel offences | - | - | 7 | - | - | - | - | - | - | - | - | - | - | - | - | - | - | 7 |
| Child pornography offences | - | - | 10 | - | - | - | - | - | - | 6 | - | - | - | - | - | - | - | 16 |
| Conspire/aid/abet serious offence | - | - | - | - | - | - | - | - | 16 | 35 | - | - | 1 | 9 | - | - | - | 61 |
| Cybercrime offences | - | - | 4 | - | - | - | - | - | - | 1 | - | - | - | - | - | - | - | 5 |
| Kidnapping | - | - | - | - | - | - | - | - | 9 | 46 | - | - | 2 | - | - | 11 | - | 68 |
| Loss of life or personal injury | - | - | 21 | - | - | - | - | - | 12 | 465 | - | - | 5 | - | - | 19 | 14 | 536 |
| Money laundering | - | - | 191 | - | - | - | - | - | 50 | 2 | - | 18 | - | 2 | - | - | 1 | 264 |
| Murder | - | - | 35 | - | - | - | - | - | 30 | 247 | 6 | - | 20 | 8 | 2 | 44 | 47 | 439 |
| Organised offences and/or criminal organisations | - | - | 27 | - | - | - | - | - | 1 | 194 | - | - | 2 | - | - | 3 | 13 | 240 |
| People smuggling and related | - | - | 7 | - | - | - | - | - | - | - | - | - | - | - | - | - | - | 7 |
| Serious damage to property and/or serious arson | - | - | 2 | - | - | - | - | - | 1 | 70 | - | - | - | - | - | 12 | 6 | 91 |
| Serious drug offences and/or trafficking | - | 2 | 629 | 13 | - | 6 | - | - | 89 | 846 | 35 | 7 | 212 | 84 | 13 | 57 | 185 | 2,178 |
| Serious fraud | - | - | 69 | 3 | - | 10 | 1 | - | - | 73 | - | 4 | - | - | - | 1 | 1 | 162 |
| Serious loss of revenue | - | - | 29 | - | - | - | - | - | - | - | - | - | - | - | - | - | - | 29 |
| Terrorism offences | - | - | 230 | - | - | - | - | - | - | 3 | - | - | 1 | - | - | - | 7 | 241 |
| **Total** | **260** | **11** | **1,314** | **27** | **25** | **20** | **13** | **8** | **208** | **1,988** | **41** | **71** | **243** | **108** | **15** | **150** | **283** | **4,785** |

## Eligibility to issue an interception warrant

An interception warrant may only be issued by an eligible judge or a nominated Administrative Appeals Tribunal (AAT) member. Table 2 records that, as of January 2017, there were 89 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
- Family Court of Australia, and
- 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: Number of Federal Court Judges, Family Court Judges, Federal Circuit Court Judges and nominated AAT Members to issue telecommunications interception warrants as of January 2017—s. 103(ab)**

| Issuing authority | Number eligible |
|---|---|
| Federal Court judges | 16 |
| Family Court judges | 4 |
| Federal Circuit Court judges | 34 |
| Nominated AAT members | 35 |

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

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

## Applications for and issue of telecommunications interception warrants

Table 3 sets out information detailing which authorities issued warrants to each of the interception agencies in the reporting period. In 2015–16, issuing authorities issued 3,857 interception warrants, a decrease of around 1 per cent from 2014–15, when 3,926 warrants were issued.

**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 Circuit Court Judges | Federal Court Judges | Nominated AAT members |
| ACLEI | - | 5 | - | 1 |
| AFP | 19 | 144 | 7 | 841 |
| CCC (QLD) | - | 14 | - | 13 |
| ICAC (NSW) | - | - | - | 13 |
| ICAC (SA) | - | - | 1 | 7 |
| NSW CC | - | - | - | 165 |
| NSW Police | - | - | 47 | 1,383 |
| NT Police | - | 21 | - | 20 |
| PIC | - | - | 3 | 57 |
| QLD Police | - | 167 | - | 76 |
| SA Police | - | - | 11 | 90 |
| TAS Police | - | - | - | 15 |
| VIC Police | - | - | - | 150 |
| CCC (WA) | 24 | - | 1 | - |
| WA Police | 232 | - | - | 50 |
| ACC | 2 | 8 | 6 | 244 |
| IBAC | - | - | - | 20 |
| **Total** | **277** | **359** | **76** | **3,145** |

**Table 4: Applications, made and refused, 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 | | Renewal applications | |
|---|---|---|---|---|---|---|---|
| | | 14/15 | 15/16 | 14/15 | 15/16 | 14/15 | 15/16 |
| ACC | Made | 290 | 260 | - | - | 27 | 37 |
| | Refused | 1 | - | - | - | - | - |
| ACLEI | Made | 3 | 6 | - | - | 1 | 2 |
| AFP | Made | 856 | 1,012 | 3 | - | 243 | 284 |
| | Refused | 4 | 1 | - | - | - | 1 |
| CCC (QLD) | Made | 44 | 27 | - | - | 13 | 1 |
| CCC (WA) | Made | 25 | 25 | - | - | 7 | 7 |
| | Refused | 2 | - | - | - | - | - |
| IBAC | Made | 18 | 20 | - | 1 | 6 | 2 |
| ICAC (NSW) | Made | 5 | 13 | - | - | 2 | 6 |
| ICAC (SA) | Made | 3 | 8 | - | - | - | - |
| NSW CC | Made | 185 | 165 | - | - | 68 | 45 |
| NSW Police | Made | 1,532 | 1,430 | 40 | 30 | 252 | 262 |
| NT Police | Made | 54 | 41 | - | - | 9 | 1 |
| PIC | Made | 48 | 60 | - | - | 9 | 31 |
| QLD Police | Made | 271 | 243 | - | - | 42 | 38 |
| SA Police | Made | 85 | 101 | - | - | 3 | 6 |
| TAS Police | Made | 24 | 15 | 1 | - | 6 | 1 |
| VIC Police | Made | 174 | 150 | 1 | 14 | 9 | 9 |
| | Refused | 2 | - | - | - | - | - |
| WA Police | Made | 318 | 282 | - | - | 53 | 33 |
| **Total** | **Made** | **3,935** | **3,858** | **45** | **45** | **750** | **765** |
| | **Refused** | **9** | **1** | **-** | **-** | **-** | **1** |
| | **Issued** | **3,926** | **3,857** | **45** | **45** | **750** | **764** |

* The 2014–15 Annual Report combined the data of warrant applications that were refused and withdrawn into one category. For the purposes of this report warrant applications from the 2014–15 that were refused or withdrawn have been placed under the category of 'Refused' only.

* In 2015–16 there were no warrant applications withdrawn.

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

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

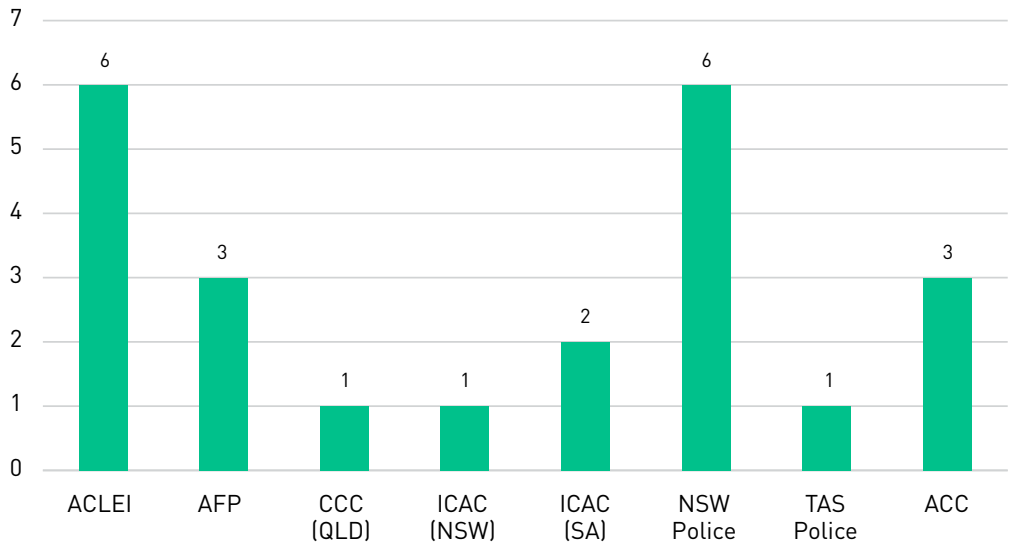
| Agency | Relevant statistics | Warrants authorising entry on premises | |
|---|---|---|---|
| | | 14/15 | 15/16 |
| AFP | Made | 1 | 2 |
| | Refused/withdrawn | - | - |
| | Issued | - | - |
| CCC (WA) | Made | 2 | - |
| | Refused/withdrawn | - | - |
| | Issued | - | - |
| **Total** | **Made** | **3** | **2** |
| | **Refused/withdrawn** | **-** | **-** |
| | **Issued** | **-** | **-** |

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

During the reporting period, 23 interception warrants were issued with a condition or restriction.

Figure 1 provides information about how these warrants are distributed across the different interception agencies.

**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 understate the effectiveness of interception as prosecutions may be initiated and convictions recorded, without the need to give intercepted information in evidence. In particular, agencies continue to report that telecommunications interception effectively enables investigators to identify persons involved in and the infrastructure of, organised criminal activities. In some cases, the weight of evidence obtained through telecommunications interception results in defendants entering guilty pleas, thereby eliminating the need for the intercepted information to be admitted into evidence.

In 2015–16 there were 3,019 arrests based on lawfully intercepted information (this figure includes instances were lawfully intercepted information culminated in an arrest). There were also 3,726 prosecutions and 1,812 convictions where lawfully intercepted material was given in evidence. Tables 6, 7 and 8 provide this information.

In previous reporting years, arresting agencies and non-arresting agencies which used lawfully intercepted information to assist in an arrest both recorded the number of 'arrests' made. In the 2015–16 reporting year agencies were asked to report on the number of times lawfully intercepted information culminated in an arrest separately from arrest numbers. This change removes the risk that arrest numbers will be duplicated.

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

| Agency | 14/15 | 15/16 | |
|---|---|---|---|
| | Number of Arrests | | Number of times lawfully intercepted information culminated in an arrest |
| ACC | 104 | - | 152 |
| ACLEI | 5 | - | 3 |
| AFP | 281 | 210 | 82 |
| CCC (WA) | - | - | - |
| CCC (QLD) | 46 | 48 | 7 |
| IBAC | - | - | 1 |
| NSW CC | 102 | - | 54 |
| NSW Police | 1,171 | 1,291 | - |
| NT Police | 35 | 35 | - |
| PIC | 9 | 2 | 1 |
| QLD Police | 457 | 428 | - |
| SA Police | 159 | 86 | 3 |
| TAS Police | 31 | 5 | - |
| VIC Police | 329 | 242 | 2 |
| WA Police | 371 | 367 | - |
| **Total** | **3,100** | **2,714** | **305** |

**Table 7: Prosecutions per offence category in which lawfully intercepted information was given in evidence**

| Categories of offences | ACC | ACLEI | AFP | CCC (QLD) | NSW CC | NSW Police | NT Police | PIC | QLD Police | SA Police | VIC Police | WA Police | TOTAL |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ACC special investigations | 3 | - | - | - | - | - | - | - | - | - | - | - | 3 |
| Administration of justice | - | - | - | - | - | - | - | - | - | - | 2 | - | 2 |
| Assisting person to escape or dispose of proceeds | - | - | - | - | - | 2 | - | - | - | - | 2 | - | 4 |
| Bribery or corruption | - | - | 2 | - | - | - | - | - | - | - | - | - | 2 |
| Child pornography offences | - | - | 1 | - | - | - | - | - | - | - | - | - | 1 |
| Conspire/aid/abet serious offence | - | - | - | - | - | - | - | 4 | - | - | 6 | - | 10 |
| Cybercrime offences | - | - | - | - | - | 100 | - | - | - | - | - | - | 100 |
| Kidnapping | - | - | - | - | - | 4 | - | - | - | - | 4 | - | 8 |
| Loss of life | - | - | - | - | - | - | - | - | - | - | 12 | - | 12 |
| Money laundering | - | - | 15 | - | 35 | 3 | - | - | - | 2 | 5 | 3 | 63 |
| Murder | - | - | - | - | 12 | 10 | 2 | - | 3 | 1 | 10 | 6 | 44 |
| Offences involving planning and organisation | - | - | - | - | - | 136 | - | - | - | - | - | 280 | 416 |
| Organised crime | - | - | 4 | - | - | 1 | - | - | - | - | - | - | 5 |
| People smuggling and related | - | - | 1 | - | - | - | - | - | - | - | - | - | 1 |
| Serious arson | - | - | - | - | - | - | - | - | - | - | - | 5 | 5 |
| Serious damage to property | - | - | - | - | - | - | - | - | - | - | - | 16 | 16 |
| Serious drug offences | - | - | 44 | - | - | 78 | 27 | - | - | - | - | - | 149 |
| Serious drug offences and/or trafficking | - | - | 86 | - | - | - | - | - | - | - | - | - | 86 |

| Categories of offences | ACC | ACLEI | AFP | CCC (QLD) | NSW CC | NSW Police | NT Police | PIC | QLD Police | SA Police | VIC Police | WA Police | TOTAL |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Serious fraud | - | - | 17 | 2 | - | 202 | - | - | 1 | 3 | - | 9 | 234 |
| Serious loss of revenue | - | - | 3 | - | - | - | - | - | - | - | - | - | 3 |
| Serious personal injury | - | - | - | - | 3 | 48 | - | - | - | - | 45 | 12 | 108 |
| Terrorism offences | - | - | 8 | - | 4 | - | - | - | - | - | - | - | 12 |
| Trafficking in prescribed substances | - | - | 18 | 1 | 222 | 557 | - | - | 32 | 50 | 156 | 979 | 2,015 |
| Other Serious Offences | - | 1 | 37 | 15 | - | 190 | - | 16 | 31 | 3 | 134 | - | 427 |
| **Total** | **3** | **1** | **236** | **18** | **276** | **1,331** | **29** | **20** | **67** | **59** | **376** | **1,310** | **3,726** |

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

| Categories of offences | ACC | ACLEI | AFP | CCC (QLD) | CCC (WA) | NSW CC | NSW Police | NT Police | PIC | QLD Police | SA Police | VIC Police | WA Police | TOTAL |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ACC special investigations | 2 | - | - | - | - | - | - | - | - | - | - | - | - | 2 |
| Administration of justice | - | - | - | - | - | - | - | - | - | - | - | 2 | - | 2 |
| Assisting person to escape or dispose of proceeds | - | - | - | - | - | - | 2 | - | - | - | - | - | - | 2 |
| Child pornography offences | - | - | 1 | - | - | - | 2 | - | - | - | - | - | - | 3 |
| Conspire/aid/abet serious offence | - | - | - | - | - | - | 2 | - | 3 | - | - | 3 | - | 8 |
| Cybercrime offences | - | - | - | - | 22 | - | - | - | - | - | - | - | - | 22 |
| Kidnapping | - | - | - | - | - | - | - | - | - | - | - | 3 | - | 3 |
| Loss of life | - | - | - | - | - | - | - | - | - | - | - | 7 | - | 7 |

| Categories of offences | ACC | ACLEI | AFP | CCC (QLD) | CCC (WA) | NSW CC | NSW Police | NT Police | PIC | QLD Police | SA Police | VIC Police | WA Police | TOTAL |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Money laundering | - | - | 4 | - | - | 19 | 6 | - | - | - | 2 | 3 | 1 | 35 |
| Murder | - | - | - | - | - | 3 | 3 | - | - | 3 | 1 | 8 | 3 | 21 |
| Offences involving planning and organisation | - | - | - | - | - | - | 26 | - | - | - | - | - | 187 | 213 |
| Organised crime | - | - | - | - | - | - | 18 | - | - | - | - | - | - | 18 |
| Serious arson | - | - | - | - | - | - | 33 | - | - | - | - | - | 2 | 35 |
| Serious damage to property | - | - | - | - | - | - | - | - | - | - | - | - | 9 | 9 |
| Serious drug offences | - | - | 6 | - | - | - | 53 | 18 | - | - | - | - | - | 77 |
| Serious drug offences and/or trafficking | - | - | 22 | - | - | - | - | - | - | - | - | - | - | 22 |
| Serious fraud | - | - | 3 | - | - | - | 13 | - | - | 1 | 3 | - | 4 | 24 |
| Serious personal injury | - | - | - | - | - | 3 | 42 | - | - | - | - | 26 | 5 | 76 |
| Terrorism offences | - | - | 4 | - | - | - | - | - | - | - | - | - | - | 4 |
| Trafficking in prescribed substances | - | - | 7 | 2 | - | 114 | 161 | - | - | 32 | 35 | 103 | 658 | 1,112 |
| Other serious offences | - | 1 | 31 | 5 | - | - | 25 | - | 16 | 31 | 4 | 4 | - | 117 |
| **Total** | **2** | **1** | **78** | **7** | **22** | **139** | **386** | **18** | **19** | **67** | **45** | **159** | **869** | **1,812** |

## Named person warrants

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

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

The following tables and figures show that in 2015–16, 964 named person warrants were issued, a decrease from the 2014–15 reporting period in which 1,000 named person warrants were issued.

In 2015–16, six named person warrants were issued with a condition or restriction, three to the AFP and three to ACC.

**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 | |
|---|---|---|---|---|---|---|---|
| | | 14/15 | 15/16 | 14/15 | 15/16 | 14/15 | 15/16 |
| ACC | Made | 185 | 184 | - | - | 23 | 34 |
| AFP | Made | 335 | 388 | 1 | - | 110 | 157 |
| | Refused | 2 | - | - | - | - | - |
| CCC (QLD) | Made | 26 | 3 | - | - | 11 | - |
| CCC (WA) | Made | 2 | 3 | - | - | - | 3 |
| IBAC | Made | 2 | 1 | - | 1 | 1 | - |
| NSW CC | Made | 91 | 70 | - | - | 47 | 22 |
| NSW Police | Made | 144 | 120 | 2 | - | 39 | 25 |
| NT Police | Made | - | 2 | - | - | - | - |
| QLD Police | Made | 46 | 49 | - | - | 6 | 8 |
| SA Police | Made | 3 | 19 | - | - | - | 2 |
| TAS Police | Made | 5 | 7 | - | - | 1 | 1 |
| VIC Police | Made | 44 | 46 | - | 3 | 3 | 5 |
| WA Police | Made | 119 | 72 | - | - | 32 | 9 |

| Agency | Relevant statistics* | Applications for named person warrants | | Telephone applications for named person warrants | | Renewal applications for named person warrants | |
|---|---|---|---|---|---|---|---|
| | | 14/15 | 15/16 | 14/15 | 15/16 | 14/15 | 15/16 |
| **Total** | **Made** | **1,002** | **964** | **3** | **4** | **273** | **266** |
| | **Refused/Withdrawn** | **2** | **-** | **-** | **-** | **-** | **-** |
| | **Issued** | **1,000** | **964** | **3** | **4** | **273** | **266** |

* The 2014–15 Annual Report combined the data of warrant applications that were refused and withdrawn into one category. For the purposes of this report warrant applications from the 2014–15 that were refused or withdrawn have been placed under the category of 'Refused' only.

* In 2015–16 there were no warrant applications withdrawn or refused.

Consistent with the last reporting period, in 2015–16 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 | |
| | 14/15 | 15/16 | 14/15 | 15/16 | 14/15 | 15/16 | 14/15 | 15/16 |
| ACC | 50 | 67 | 123 | 95 | 18 | 16 | 8 | 3 |
| ACLEI | - | - | - | - | - | - | - | - |
| AFP | 104 | 119 | 205 | 244 | 21 | 20 | 1 | - |
| CCC (QLD) | 7 | 1 | 15 | 2 | 3 | - | - | - |
| CCC (WA) | - | - | 1 | 1 | - | - | 1 | 2 |
| IBAC | - | - | 1 | 1 | 1 | - | - | - |
| NSW CC | 36 | 26 | 47 | 39 | 6 | 4 | 1 | - |
| NSW Police | 33 | 25 | 95 | 92 | 10 | 2 | - | 1 |
| NT Police | - | - | - | 2 | - | - | - | - |
| QLD Police | 10 | 9 | 32 | 32 | 4 | 8 | - | - |
| SA Police | - | 5 | 3 | 14 | - | - | - | - |
| TAS Police | - | 1 | 4 | 1 | 2 | 5 | - | - |
| VIC Police | 10 | 9 | 28 | 32 | 2 | 5 | 1 | - |
| WA Police | 33 | 16 | 78 | 54 | 8 | 2 | - | - |
| **Total** | **283** | **278** | **632** | **609** | **75** | **62** | **12** | **6** |

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.

Subparagraphs 100(1)(ec)(i)-(iii) require the report to include the total number of:

(i) services intercepted under service based named person warrants

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

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

Figure 2 and Table 11 outline the number of services intercepted under the different types of named person warrants and should be read in conjunction with Table 9, which provides the total number of named person warrants issued.

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

Table 11 shows, consistent with previous years, that in 2015–16, device-based named person warrants were used by only a small number of agencies.

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

| Agency | Services | Devices |
|---|---|---|
| ACC | 57 | 32 |
| AFP | 342 | 145 |
| NSW Police | 8 | 10 |
| WA Police | 2 | - |
| **Total** | **409** | **187** |

## 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 2015–16, 108 B-Party warrants were issued, a slight increase on the 102 B Party warrants issued in 2014–15. There were no withdrawn applications for B-Party warrants in 2015–16.

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

| Agency | Relevant statistics | Applications for B-Party warrants | | Telephone applications for B-Party warrants | | Renewal applications for B-Party warrants | |
|---|---|---|---|---|---|---|---|
| | | 14/15 | 15/16 | 14/15 | 15/16 | 14/15 | 15/16 |
| ACC | Made | 4 | - | - | - | 1 | - |
| AFP | Made | 50 | 60 | - | - | 32 | 26 |
| | Refused | - | 1 | - | - | - | 1 |
| NSW CC | Made | 7 | 4 | - | - | - | - |
| NSW Police | Made | 41 | 43 | 9 | 9 | - | - |
| QLD Police | Made | - | 2 | - | - | - | - |
| **Total** | **Made** | **102** | **109** | **9** | **9** | **33** | **26** |
| | **Refused** | **-** | **1** | **-** | **-** | **-** | **1** |
| | **Issued** | **102** | **108** | **9** | **9** | **33** | **25** |

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

| Agency | Applications for B-Party warrants | |
|---|---|---|
| | 14/15 | 15/16 |
| AFP | 2 | - |
| NSW Police | 1 | 1 |
| **Total** | **3** | **1** |

## 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 in the reporting period.

**Table 14: Duration of original and renewal telecommunications interception warrants—ss. 101(1)(a)-(d) and 101(2)(a)-(d)**

| Agency | Duration of original telecommunications interception warrants | | Duration of renewal of telecommunications interception warrants | |
|---|---|---|---|---|
| | Average period specified in warrants (days) | Average period warrants in force (days) | Average period specified in warrants (days) | Average period warrants in force (days) |
| ACC | 89 | 61 | 89 | 69 |
| ACLEI | 90 | 88 | 90 | 89 |
| AFP | 80 | 55 | 83 | 72 |
| CCC (QLD) | 65 | 58 | 59 | 59 |
| CCC (WA) | 82 | 51 | 81 | 66 |
| IBAC | 76 | 67 | 67 | 12 |
| ICAC (NSW) | 90 | 78 | 79 | 64 |
| ICAC (SA) | 74 | 45 | - | - |
| NSW CC | 82 | 72 | 86 | 71 |
| NSW Police | 54 | 39 | 59 | 45 |
| NT Police | 87 | 52 | 87 | 33 |
| PIC | 84 | 74 | 87 | 78 |
| QLD Police | 75 | 56 | 75 | 59 |
| SA Police | 73 | 52 | 72 | 74 |
| TAS Police | 76 | 54 | 90 | 56 |
| VIC Police | 83 | 51 | 46 | 29 |
| WA Police | 90 | 58 | 90 | 72 |
| **Average** | **79** | **59** | **78** | **58** |

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 in the reporting period.

**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) |
| AFP | 44 | 41 | 45 | 44 |
| NSW CC | 29 | 16 | - | - |
| NSW Police | 31 | 18 | - | - |
| QLD Police | 10 | 10 | - | - |
| **Average** | **29** | **21** | **45** | **44** |

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

The categories of final renewals are:

- 90 day final renewal—a last renewal that ceases to be in force more than 90 days but not more than 150 days after the date of issue of the original warrant
- 150 day final renewal—a last renewal that ceases to be in force more than 150 days but not more than 180 days after the date of issue of the original warrant, and
- 180 day final renewal—a last renewal that ceases to be in force more than 180 days after the date of issue of the original warrant.

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

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

| Agency | 90 days | | 150 days | | 180 days | |
|---|---|---|---|---|---|---|
| | 14/15 | 15/16 | 14/15 | 15/16 | 14/15 | 15/16 |
| ACC | 8 | 7 | 8 | 15 | 6 | 5 |
| ACLEI | - | - | - | - | - | 1 |
| AFP | 35 | 26 | 51 | 46 | 68 | 42 |
| CCC (QLD) | 2 | - | 8 | - | - | - |
| CCC (WA) | 1 | 2 | 6 | 3 | - | 1 |
| IBAC | - | 1 | 4 | 1 | 1 | - |
| ICAC (NSW) | 2 | 1 | - | 1 | - | 1 |
| NSW CC | 3 | 6 | 18 | 4 | 20 | 5 |
| NSW Police | 110 | 137 | 8 | 16 | 30 | 16 |
| NT Police | - | 1 | 3 | - | 2 | - |
| PIC | 3 | 1 | - | 6 | - | 5 |
| QLD Police | 13 | 14 | 12 | 12 | 4 | 3 |
| SA Police | 3 | 2 | - | 2 | - | - |
| TAS Police | - | 1 | - | - | - | - |
| VIC Police | - | 5 | - | 3 | - | - |
| WA Police | 11 | 4 | 23 | 12 | 12 | 6 |
| **Total** | **191** | **208** | **141** | **121** | **143** | **85** |

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

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

| Agency | Total number of warrants | Number of eligible warrants | % |
|---|---|---|---|
| ACC | 250 | 173 | 69 |
| ACLEI | 6 | 4 | 67 |
| AFP | 1,154 | 727 | 63 |
| CCC (QLD) | 31 | 20 | 65 |
| CCC (WA) | 34 | 2 | 6 |
| IBAC | 25 | 10 | 40 |
| ICAC (NSW) | 12 | 10 | 83 |
| ICAC (SA) | 10 | - | - |
| NSW CC | 192 | 136 | 71 |
| NSW Police | 1,541 | 1,131 | 73 |
| NT Police | 35 | 23 | 66 |
| PIC | 24 | 18 | 75 |
| QLD Police | 277 | 266 | 96 |
| SA Police | 107 | 69 | 64 |
| TAS Police | 17 | 12 | 71 |
| VIC Police | 171 | 128 | 75 |
| WA Police | 293 | 172 | 59 |
| **TOTAL** | **4,179** | **2,901** | **69** |

## 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 18 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. There were no cases where an officer of the agency undertaking the interception was a party to the communication.

**Table 18: 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 | |
| | 14/15 | 15/16 | 14/15 | 15/16 | 14/15 | 15/16 | 14/15 | 15/16 |
| NSW Police | - | 11 | - | 11 | - | - | - | - |
| **Total** | **-** | **11** | **-** | **11** | **-** | **-** | **-** | **-** |

## Mutual assistance

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

## Number of interceptions carried out on behalf of other agencies

The TIA Act supports the ability of interception agencies to cooperate and to work collaboratively by enabling one interception agency to carry out interception on behalf of other agencies.

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

| Interception carried out by: | Interception carried out on behalf of: | Number of interceptions: |
|---|---|---|
| ACC | CCC (QLD) | 27 |
| | SA Police | 5 |
| AFP | ACLEI | 6 |
| | ACC | 8 |
| | NSW Police | 1 |
| CCC (WA) | WA Police | 1 |
| | IBAC | 8 |
| VIC Police | TAS Police | 14 |
| IBAC | ICAC (SA) | 8 |
| **TOTAL** | | **78** |

## Telecommunications interception expenditure

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

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

| Agency | Total expenditure ($) | Average expenditure ($) |
|---|---|---|
| ACC | 8,093,128 | 31,127 |
| ACLEI | 342,594 | 57,099 |
| AFP | 16,746,407 | 16,564 |
| CCC (QLD) | 1,805,614 | 66,874 |
| CCC (WA) | 2,218,804 | 88,752 |
| IBAC | 1,722,724 | 86,136 |
| ICAC (NSW) | 155,522 | 11,963 |
| ICAC (SA) | 168,346 | 21,043 |
| NSW CC | 2,300,050 | 13,939 |
| NSW Police | 7,239,911 | 5,062 |
| NT Police | 1,105,872 | 9,657 |
| PIC | 1,546,914 | 25,781 |
| QLD Police | 11,216,457 | 46,158 |
| SA Police | 3,775,436 | 37,380 |
| TAS Police | 607,000 | 37,333 |
| VIC Police | 7,719,442 | 51,462 |
| WA Police | 3,624,454 | 12,852 |
| **TOTAL** | **70,388,675** | **619,182** |

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 interception costs per agency**

| Agency | Salaries | Administrative support | Capital expenditure | Interception costs | Total ($) |
|---|---|---|---|---|---|
| ACC | 6,074,026 | 202,317 | 598,065 | 1,218,720 | 8,093,128 |
| ACLEI | 211,347 | 102,446 | - | 28,801 | 342,594 |
| AFP | 11,240,814 | 888,234 | 2,797,896 | 1,819,463 | 16,746,407 |
| CCC (QLD) | 1,113,532 | 204,468 | 55,000 | 432,614 | 1,805,614 |
| CCC (WA) | 1,089,576 | 1,189 | 1,048,362 | 79,677 | 2,218,804 |
| IBAC | 1,465,290 | 27,220 | 61,137 | 169,077 | 1,722,724 |
| ICAC (NSW) | 52,200 | - | - | 103,322 | 155,522 |
| ICAC (SA) | 85,248 | - | - | 83,098 | 168,346 |
| NSW CC | 1,864,319 | - | - | 435,731 | 2,300,050 |
| NSW Police | 5,597,331 | 231,351 | - | 1,411,229 | 7,239,911 |
| NT Police | 709,910 | - | 20,000 | 375,962 | 1,105,872 |
| PIC | 1,308,417 | - | - | 238,497 | 1,546,914 |
| QLD Police | 4,541,087 | 893,356 | 5,043,547 | 738,466 | 11,216,456 |
| SA Police | 2,522,280 | 363,459 | 216,173 | 673,524 | 3,775,436 |
| TAS Police | 557,000 | - | - | 50,000 | 607,000 |
| VIC Police | 5,882,921 | 47,661 | 415,814 | 1,373,047 | 7,719,443 |
| WA Police | 3,172,700 | 302,629 | - | 149,125 | 3,624,454 |
| **TOTAL** | **47,487,998** | **3,264,330** | **10,255,994** | **9,380,353** | **70,388,675** |

## Emergency service facilities

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

**Table 22: Emergency service facility declarations**

| State/territory | Police | Fire brigade | Ambulance | Emergency services authority | Dispatching |
|---|---|---|---|---|---|
| Australian Capital Territory | 5 | - | - | - | 3 |
| New South Wales | 8 | 95 | 6 | - | 6 |
| Northern Territory | 2 | - | 1 | 1 | 4 |
| Queensland | 21 | 12 | 9 | - | 13 |
| South Australia | 1 | 2 | 1 | - | 3 |
| Tasmania | 1 | 2 | 1 | - | 2 |
| Victoria | 6 | 1 | 10 | - | 8 |
| Western Australia | 1 | 2 | 1 | - | 6 |
| **Total** | **45** | **114** | **29** | **1** | **45** |

## Safeguards and reporting requirements on interception powers

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. These include a requirement for:

- the heads of interception agencies to provide the Secretary of the Attorney-General's Department (AGD) with a copy of each telecommunications interception warrant
- interception agencies to 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 to maintain 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 to maintain a Special Register recording the details of telecommunications interception warrants that do not lead to a prosecution within three months of the warrant expiring. The Special Register is also given to the Attorney-General to inspect.

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

At least twice a year the Commonwealth Ombudsman must inspect the records kept by the ACC, ACLEI and the AFP relating to interceptions and the use, dissemination and destruction of intercepted information. The inspections are retrospective and on the basis of a full year, and for this reason, the Ombudsman inspected relevant telecommunications interception warrants that were expired or revoked in the period between 1 January and 31 December 2015.

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 inspections of records in relation to access by enforcement agencies (including both Commonwealth and state agencies) to stored communications and telecommunications data. The Data Retention Act introduced additional obligations for these reports to be provided to the Attorney-General and tabled in Parliament.

## Commonwealth Ombudsman—inspection of telecommunications interception records

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

During its review of warrants that expired or revoked in the period between 1 January and 31 December 2015 the Ombudsman noted that there continues to be a high level of compliance with the TIA Act, where agencies displayed a good understanding of the TIA Act's requirements. The Ombudsman noted agency responsiveness towards inspection findings.

Overall, the Ombudsman did not identify any systemic issues or significant problems, with all agencies found to be compliant with the majority of the Ombudsman's inspection criteria. The Ombudsman's inspection criteria (see Figures 3 and 4) are:

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

## Commonwealth Ombudsman's summary of findings

**Table 23: Summary of findings from the two inspections conducted at each agency between 1 January and 31 December 2015**

| CRITERIA | ACC | ACLEI | AFP |
|---|---|---|---|
| Were restricted records properly destroyed (s 79)? | Not assessed. The ACC advised it did not conduct any destructions of restricted records during the inspection period. | Compliant. | Non-compliant. A number of restricted records were not destroyed as required. The AFP has amended its destruction procedures in line with Ombudsman suggestions. |
| Were the requisite documents kept in connection with the issue of warrants (s 80)? | Compliant. | Compliant. | Compliant. |
| Were warrants properly applied for and in the correct form (ss 39(1) and 49)? | Nothing to indicate otherwise. | Nothing to indicate otherwise. | Compliant with the exception of two instances. Despite this the Ombudsman notes that the AFP procedures are sufficient. |
| Were requisite records kept in connection with interceptions (s 81)? | Compliant. | Compliant. | Compliant. |
| Were interceptions conducted in accordance with the warrants (s 7) and was any unlawfully intercepted information properly dealt with (s 63)? | Compliant. | Compliant. | Compliant with the exception of two instances. |

## Commonwealth Ombudsman's findings per Commonwealth agency for warrants expiring between 1 January to 31 December 2015

### ACC

No formal recommendations were made as a result of either of the two inspections of the ACC. In response to a self-disclosed instance where a warrant was issued for a longer period than allowed for under the Act, the Ombudsman made a suggestion to improve compliance. The ACC acknowledged the error and advised that it implemented the suggested improvement to internal guidelines.

The Ombudsman noted the ACC had taken appropriate remedial action to address issues identified in previous inspections. The Ombudsman also noted that the ACC's policies and procedures are working as intended to prevent unlawfully intercepted information being disseminated to investigators.

### ACLEI

No formal recommendations or suggestions were made as a result of either of the two inspections of ACLEI. The Ombudsman noted that ACLEI was cooperative and forthcoming with information at the inspection.

### AFP

No formal recommendations were made as a result of either of the two inspections of the AFP. However the Ombudsman noted that the AFP was not compliant in a number of instances in relation to its destruction obligations. The Ombudsman suggested that the AFP update its procedures and processes to ensure compliance with section 79(1) of the TIA Act. The AFP accepted the suggestion and advised the Ombudsman that it has changed is destruction procedures.

The Ombudsman noted two instances where warrants were not in the prescribed form as required by s 49(1) of the TIA Act. Given that the frequency of non-compliance with this requirement has decreased over time, the Ombudsman concluded that the AFP's procedures in relation to the matter are sufficient to achieve compliance with the Act.

The Ombudsman noted in two instances that the AFP was non-compliant with interception requirements. However, the AFP has been able to quarantine unlawfully intercepted information prior to disseminating the product to investigations. Despite these findings the Ombudsman remains of the view that the AFP's procedures relating to the lawful interception of communications are sufficient to achieve compliance with the Act.

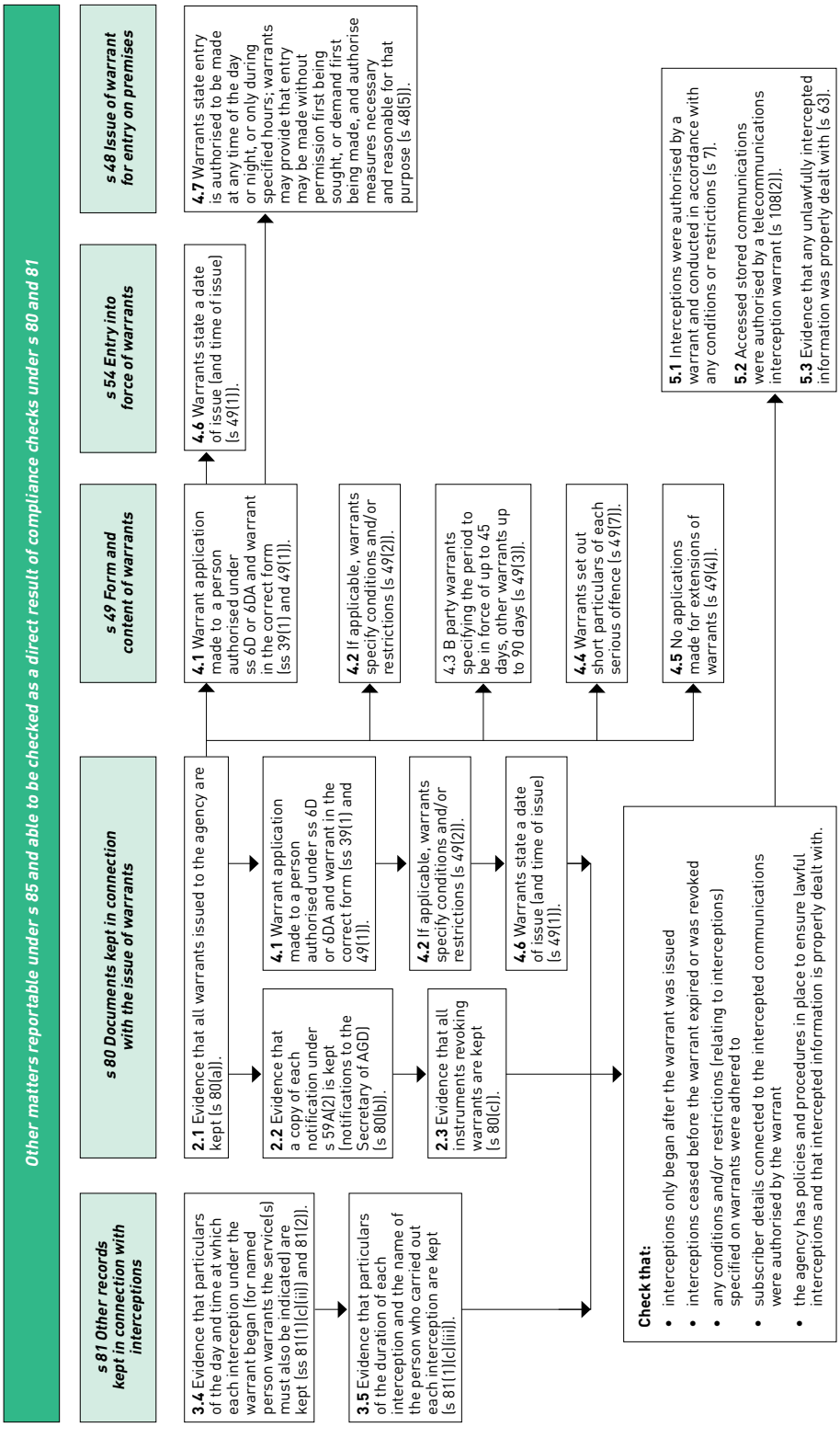
Further information about the Commonwealth Ombudsman's telecommunications interception inspection criteria is outlined in Figure 3 and 4 below.

**Figure 3: 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* | *s 80 Documents kept in connection with the issue of warrants* | *s 81 Other records kept in connection with interceptions (Warrant details, lawfully intercepted information (LII) records, use and communication)* |
|---|---|---|
| **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)).<br>**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)). | **2.1** Evidence that all warrants issued to the agency are kept (s 80(a)).<br>**2.2** Evidence that a copy of each notification under s 59A(2) is kept (notifications to the Secretary of AGD) (s 80(b)).<br>**2.3** Evidence that all instruments revoking warrants are kept (s 80(c)).<br>**2.4** Evidence that a copy of each certificate issued under s 61(4) is kept (*evidentiary certificates*) (s 80(d)).<br>**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)). | **3.1** Evidence that each telephone application for a part 2–5 warrant is kept (s 81(1)(a)).<br>**3.2** Evidence that statements as to whether applications were withdrawn, refused or issued on the application are kept (s 81(1)(a)).<br>**3.3** Evidence that the particulars of all warrants whose authority is exercised by the agency are kept (s 81(1)(c)(i)).<br>**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)).<br>**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)).<br>**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)).<br>**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)).<br>**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)).<br>**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)).<br>**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)).<br>**3.11** Evidence that particulars of each use made by the agency of LII are kept (s 81(1)(e)).<br>**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)).<br>**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 4: Other matters reportable under s. 85**



# CHAPTER 2

## STORED COMMUNICATIONS

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

**Definition**

**All 'criminal law-enforcement agencies' are set out in section 110A of the TIA Act. These agencies include all interception agencies as well as the Department of Immigration and Border Protection, the Australian Securities and Investments Commission and the Australian Competition and Consumer Commission.**

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

**Definition**

**A 'serious contravention' includes:**

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

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

| Agency | Relevant statistics* | Applications for stored communications warrants | | Telephone applications for stored communications warrants | |
|---|---|---|---|---|---|
| | | 14/15 | 15/16 | 14/15 | 15/16 |
| ACC | Made | 4 | 2 | - | - |
| ACCC | Made | 4 | - | - | - |
| AFP | Made | 94 | 80 | - | - |
| ASIC | Made | - | 1 | - | - |
| CCC (QLD) | Made | - | 3 | - | - |
| CCC (WA) | Made | - | 5 | - | - |
| DIBP | Made | 10 | 1 | - | - |
| NSW CC | Made | 3 | 4 | - | - |
| NSW Police | Made | 290 | 345 | - | - |
| NT Police | Made | 16 | 11 | - | - |
| PIC | Made | 7 | 16 | - | - |
| QLD Police | Made | 123 | 132 | - | - |
| SA Police | Made | 38 | 19 | - | - |
| TAS Police | Made | 30 | 17 | - | - |
| | Refused | 1 | - | - | - |
| VIC Police | Made | 40 | 41 | - | - |
| WA Police | Made | 38 | 35 | - | - |
| **Total** | **Made** | **697** | **712** | **-** | **-** |
| | **Refused** | **1** | **-** | **-** | **-** |
| | **Issued** | **696** | **712** | **-** | **-** |

* The 2014–15 Annual Report combined the data of warrant applications that were refused and withdrawn into one category. For the purposes of this report warrant applications from the 2014–15 that were refused or withdrawn have been placed under the category of 'Refused' only.

* In 2015–16 there were no warrant applications withdrawn or refused.

**Table 25: Stored communications warrants subject to conditions or restrictions—s. 162(2)(d)**

| Agency | Application for warrants |
|---|---|
| | 15/16 |
| NSW Police | 345 |
| SA Police | 2 |
| **Total** | **347** |

## Effectiveness of stored communications warrants

In 2015–16, criminal law-enforcement agencies made 366 arrests, conducted 485 proceedings and obtained 195 convictions based on evidence obtained under stored communications warrants.

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

| Agency | Arrests | | Proceedings | | Convictions | |
|---|---|---|---|---|---|---|
| | 14/15 | 15/16 | 14/15 | 15/16 | 14/15 | 15/16 |
| ACCC | - | - | - | 1 | - | - |
| ACC | 5 | 4 | - | - | - | - |
| AFP | 46 | 12 | 34 | 7 | 15 | 5 |
| CCC (QLD) | 3 | 2 | - | 1 | - | 1 |
| NSW CC | - | 3 | - | - | - | - |
| NSW Police | 179 | 167 | 221 | 362 | 107 | 86 |
| NT Police | 8 | 7 | - | 7 | - | 2 |
| PIC | 8 | 2 | - | 7 | - | 4 |
| QLD Police | 69 | 130 | 68 | 67 | 68 | 66 |
| SA Police | 17 | 6 | 3 | - | 2 | 2 |
| TAS Police | 4 | 5 | - | - | 1 | - |
| VIC Police | 28 | 20 | 7 | 29 | 1 | 26 |
| WA Police | 10 | 8 | 2 | 4 | 4 | 3 |
| **Total** | **377** | **366** | **335** | **485** | **198** | **195** |

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

## Preservation notices

Under Part 3-1A of Chapter 3 of the TIA Act, criminal law-enforcement agencies can give a preservation notice to a carrier. A preservation notice allows criminal law-enforcement agencies to preserve stored communications that a carrier holds. The carrier is required to keep the stored communications while the notice is in force. The purpose of the notice is to preserve communications in order to support criminal law-enforcement agencies during their investigations by allowing them to seek warrants where necessary.

The TIA Act provides for three types of preservation notices:

- *historic domestic preservation notices*—requires the preservation of all communications held by the carrier on the day of the notice for up to 90 days.
- *ongoing domestic preservation notice*—requires the preservation of all communications held by the carrier for a period of 29 days from the day after the notice is received. The notice remains in force for up to 90 days.
- *foreign preservation notices*—requires the preservation of all stored communications that a carrier holds that relate to the specified person connected with the contravention of foreign laws.

Domestic preservation notices must be revoked if the person specified in the notice is no longer under investigation. A criminal law-enforcement agency must also revoke a notice if the agency decides not to apply for a warrant to access the stored communications covered by the notice.

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

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

| Agency | Domestic preservation notice issued | Domestic preservation revocation notices issued |
|---|---|---|
| ACC | 4 | - |
| ASIC | 55 | - |
| AFP | 213 | 64 |
| CCC (QLD) | 31 | 11 |
| CCC (WA) | 5 | 1 |
| DIBP | 3 | - |
| ICAC (NSW) | 2 | - |
| ICAC (SA) | 2 | - |
| NSW CC | 7 | 5 |
| NSW Police | 443 | 72 |
| NT Police | 112 | 64 |
| PIC | 27 | 5 |
| QLD Police | 295 | 157 |
| SA Police | 89 | 73 |
| TAS Police | 113 | 26 |
| VIC Police | 71 | 11 |
| WA Police | 104 | 28 |
| **Total** | **1,576** | **517** |

Under section 161A(2) of the TIA Act the AFP is required to report on foreign preservation notices. In 2015–16, the AFP reported that five foreign preservation notices and no foreign preservation notice revocation notices were issued.

## Mutual assistance

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

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 2015–16 there were no occasions on which this information was provided to a foreign country under the Mutual Assistance Act.

## Ombudsman Inspection Report

The Commonwealth Ombudsman inspects the preservation notices and stored communications access records of all criminal law-enforcement agencies. Summaries of these inspections have been included in previous annual reports.

Due to changes made through the Data Retention Act, the annual report will no longer include information on inspections concerning stored communications and preservation notices. Under new section 186J the Commonwealth Ombudsman continues to have a statutory obligation to report on the results of these inspections to the Minister. However, the Minister must now cause a copy of this report to be tabled before each House of Parliament within 15 sitting days after receipt of the inspection report. This requirement will ensure the Parliament and public have visibility of the inspection results outside of the annual report.

# 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' includes 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.**

**From 13 October 2015, the definition of enforcement agency was restricted to 20 agencies that also fall under the definition of 'criminal law-enforcement agency'. All criminal law-enforcement agencies are set out in section 110A of the TIA Act. These agencies include all interception agencies as well as the Department of Immigration and Border Protection, the Australian Securities and Investments Commission and the Australian Competition and Consumer Commission.**

In addition to restricting the number of agencies with access to telecommunications data to 21 agencies, the Data Retention Act introduced new reporting requirements from 13 October 2015.

Agencies no longer able to access telecommunications data under the TIA Act from 13 October 2015 have recorded authorisations for telecommunications data for the period between 1 July 2015 and 12 October 2015. The new reporting requirements expressed in tables 39–43 came into effect on 13 October 2015 and record relevant agency activities from 13 October 2015 to 30 June 2016.

Between 1 July 2015 and 12 October 2015, 63 enforcement agencies made historical data authorisations.

**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.

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—authorisations

Tables 28–36 provide information on the use of historical data by all enforcement agencies authorised to disclosure telecommunications data at some point within the 2015–16 reporting year.

Table 28, 32 and 36 set out the number of authorisations made by current criminal law-enforcement agencies that continued to have access to historical data under the TIA Act after the commencement of the Data Retention Act.

In 2015–16 criminal law-enforcement agencies made:

- 325,807 authorisations for access to existing information or documents to enforce the criminal law
- 2,426 authorisations for access to existing information or documents to enforce a law imposing a pecuniary penalty or to protect the public revenue, and
- 4,406 authorisations for access to existing information or documents to locate missing persons.

In total, criminal law-enforcement agencies made 332,639 authorisations for historical data.

Tables 29, 30, 33 and 34 include statistics for historical data authorisations made by enforcement agencies that were no longer able to access telecommunications data under the TIA Act as of 13 October 2015. These tables cover authorisations made from 1 July 2015 to 12 October 2015.

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

| Agency | Authorisations | |
|---|---|---|
| | 14/15 | 15/16 |
| ACC | 7,429 | 8,721 |
| ACCC | 133 | 70 |
| ASIC | 1,691 | 1,822 |
| DIBP | 9,851 | 2,622 |
| ACLEI | 5,908 | 2,123 |
| AFP | 27,462 | 25,640 |
| CCC (QLD) | 12,451 | 2,377 |
| CCC (WA) | 1,333 | 664 |
| IBAC | 424 | 240 |
| ICAC (NSW) | 532 | 261 |
| ICAC (SA) | 734 | 112 |
| NSW CC | 3,023 | 2,196 |
| NSW Police | 114,111 | 105,710 |
| NT Police | 3,391 | 2,882 |
| PIC | 1,296 | 1,479 |
| QLD Police | 40,710 | 29,271 |
| SA Police | 11,668 | 14,264 |
| TAS Police | 8,152 | 7,969 |
| VIC Police | 66,663 | 82,034 |
| WA Police | 36,310 | 35,350 |
| **Total** | **353,272** | **325,807** |

**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 for the period 1 July 2015 to 12 October 2015—s. 186(1)(a)**

| Agency | Authorisations | |
|---|---|---|
| | 14/15 | 1/7/15 – 12/10/15 |
| ATO | 206 | 35 |
| Australia Post | - | 64 |
| Australian Financial Security Authority | 76 | 16 |
| Civil Aviation Safety Authority | 11 | - |
| Clean Energy Regulator | 2 | - |
| Dept. of Agriculture | 58 | 16 |
| Dept. of Foreign Affairs and Trade | - | 11 |
| Dept. of Defence (IGD, ADFIS) | 21 | - |
| Dept. of Health | 58 | - |
| Dept. of the Environment | 21 | - |
| **Total** | **453** | **142** |

**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 for the period 1 July 2015 to 12 October 2015—s. 186(1)(a)**

| Agency | Jurisdiction | Authorisations | |
|---|---|---|---|
| | | 14/15 | 1/7/15 – 12/10/15 |
| Consumer and Business Services | SA | 111 | 110 |
| Corrective Services NSW | NSW | 52 | 6 |
| Corrections Victoria | VIC | 276 | 48 |
| Dept. of Commerce | WA | 97 | 26 |
| Dept. of Economic Development, Jobs, Transport and Resources | VIC | 226 | 173 |
| Dept. of Environment Regulation | WA | 18 | - |
| Dept. of Environment, Land, Water and Planning | VIC | 27 | 4 |
| Environment Protection Authority | NSW | 51 | 7 |
| Hume City Council | VIC | - | 1 |
| Integrity Commission | TAS | - | 4 |
| Legal Services Board | VIC | 3 | - |
| Office of Environment & Heritage | NSW | 46 | 11 |
| Roads and Maritime Services NSW | NSW | 5 | - |
| RSPCA Victoria | VIC | 133 | 23 |
| RSPCA TAS | TAS | 2 | - |
| RSPCA Queensland | QLD | 14 | 8 |
| Transport Accident Commission | VIC | 8 | 1 |
| State Insurance Regulatory Authority (Formerly Workcover NSW) | NSW | 6 | 1 |
| Worksafe Victoria | VIC | 41 | 1 |
| **Total** | | **1,116** | **424** |

**Table 31: Total number of authorisations made for access to existing information or documents in the enforcement of a criminal law—s. 186(1)(a)**

| Agency | Authorisations | |
|---|---|---|
| | 14/15 | 15/16 |
| No. of authorisations made by a Law Enforcement Agency | 341,597 | 321,293 |
| No. of authorisations made by a Commonwealth Agency[8] | 12,128 | 4,656 |
| No. of authorisations made by a State or Territory Agency[9] | 1,116 | 424 |
| **Total** | **354,841** | **326,373** |

**Table 32: Number of authorisations made by a criminal 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 | |
|---|---|---|
| | 14/15 | 15/16 |
| ACCC | 132 | 62 |
| ASIC | 160 | 110 |
| DIBP | 261 | 67 |
| AFP | 43 | 75 |
| CCC (QLD) | 3 | - |
| IBAC | - | 1 |
| NSW Police | 3,570 | 972 |
| NT Police | - | 4 |
| QLD Police | 400 | 70 |
| SA Police | 2 | 1 |
| TAS Police | 536 | 972 |
| WA Police | - | 92 |
| **Total** | **5,107** | **2,426** |

8 With the exception of ASIC, ACCC and DIBP, Commonwealth agencies only reported for the period from 1 July 2015 to 12 October 2015.

9 State and Territory Agencies only reported for the period from 1 July 2015 to 12 October 2015.

**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 pecuniary penalty or the protection of the public revenue for the period 1 July 2015 to 12 October 2015—s. 186(1)(b)**

| Agency | Authorisations | |
|---|---|---|
| | 14/15 | 1/7/15 – 12/10/15 |
| ATO | 43 | - |
| Australia Post | 625 | - |
| Australian Health Practitioner Regulation Agency | 22 | 4 |
| Department of Industry and Science (National Measurement Institute) | 1 | - |
| Dept. of Foreign Affairs and Trade | 145 | 44 |
| Dept. of Defence (IGD, ADFIS) | 71 | 15 |
| Dept. of Human Services | 269 | 34 |
| Dept. of Prime Minister & Cabinet | 1 | - |
| Dept. of Social Services | 6 | 2 |
| Fair Work Building & Construction | 8 | 1 |
| **Total** | **1,191** | **100** |

**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 for the period 1 July 2015 to 12 October 2015—s. 186(1)(b)**

| Agency | Jurisdiction | Authorisations | |
|---|---|---|---|
| | | 14/15 | 1/7/15 – 12/10/15 |
| ACT Revenue Office | ACT | 3 | - |
| Bankstown City Council | NSW | 13 | 1 |
| Consumer Affairs Victoria | VIC | 132 | 65 |
| Consumer and Business Services | SA | 21 | - |
| Dept of Environment and Heritage Protection | QLD | 28 | 3 |
| Dept. of Agriculture and Fisheries | QLD | 41 | 10 |
| Dept. of Commerce | WA | 115 | 23 |
| Dept. of Economic Development, Jobs, Transport and Resources | VIC | 1 | - |
| Dept. of Fisheries | WA | 98 | 60 |
| Dept. of Justice (Sheriffs Office of Victoria) | VIC | 3 | - |

| Agency | Jurisdiction | Authorisations | |
|---|---|---|---|
| | | 14/15 | 1/7/15 – 12/10/15 |
| Dept. of Mines and Petroleum | WA | 1 | - |
| Dept. of Parks and Wildlife | WA | 42 | 6 |
| Dept. of Primary Industries | NSW | 148 | 41 |
| Harness Racing New South Wales | NSW | 15 | 1 |
| Harness Racing Victoria | VIC | 2 | - |
| Health Care Complaints Commission | NSW | 63 | 20 |
| Ipswich City Council | QLD | 3 | - |
| Juvenile Justice NSW | NSW | 2 | - |
| Knox City Council | VIC | 15 | 11 |
| Office of Fair Trading | NSW | 675 | 179 |
| Office of Fair Trading | QLD | 361 | 87 |
| Office of Liquor and Gaming Regulation | QLD | 2 | - |
| Office of State Revenue | NSW | 34 | 4 |
| Office of State Revenue | QLD | 1 | - |
| Office of the Racing Integrity Commissioner | VIC | 48 | - |
| Primary Industries & Regions | SA | 238 | 77 |
| Racing and Wagering Western Australia | WA | 7 | 6 |
| Racing NSW | NSW | 33 | 77 |
| Racing Queensland | QLD | 5 | - |
| Revenue SA | SA | 10 | 2 |
| State Revenue Office Victoria | VIC | 32 | 2 |
| Taxi Services Commission | VIC | 5 | - |
| **Total** | | **2,197** | **675** |

**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 | |
|---|---|---|
| | 14/15 | 15/16 |
| No. of authorisations made by a Law Enforcement Agency | 4,554 | 2,187 |
| No. of authorisations made by a Commonwealth Agency[10] | 1,744 | 339 |
| No. of authorisations made by a State or Territory Agency[11] | 2,197 | 675 |
| **Total** | **8,495** | **3,201** |

**Table 36: Number of authorisations made for access to existing information or documents for the location of missing persons—s. 186(1)(aa)**

| Agency | Authorisations | |
|---|---|---|
| | 14/15 | 15/16 |
| AFP | 112 | 96 |
| NSW Police | 1,377 | 1,597 |
| NT Police | 8 | 12 |
| QLD Police | 639 | 796 |
| SA Police | 50 | 147 |
| TAS Police | 201 | 175 |
| VIC Police | 5 | 1,513 |
| WA Police | - | 70 |
| **Total** | **2,392** | **4,406** |

10 With the exception of ASIC, ACCC and DIBP, Commonwealth agencies only reported for the period from 1 July 2015 to 12 October 2015.

11 State and Territory Agencies only reported for the period from 1 July 2015 to 12 October 2015.

## Prospective data—authorisations

Tables 37 and 38 set out information about the use of prospective data authorisations during the reporting year. The number of authorisations made by a criminal law-enforcement agency for access to specified information or documents that come into existence during the period for which an authorisation is in force is contained in Table 37.

**Table 37: Prospective data authorisations—s. 186(1)(c)**

| Agency | Number of authorisations made | Days specified in force | Actual days in force | Authorisations discounted |
|---|---|---|---|---|
| ACC | 2,163 | 40,931 | 31,265 | 91 |
| ACLEI | 87 | 3315 | 3,270 | 1 |
| AFP | 2,592 | 98,164 | 56,579 | 208 |
| CCC (QLD) | 218 | 5,743 | 3,055 | 9 |
| CCC (WA) | 37 | 1,587 | 1,166 | 4 |
| DIBP | 167 | 232 | 211 | - |
| IBAC | 134 | 5,568 | 4,707 | 5 |
| ICAC (NSW) | 2 | 90 | 46 | - |
| ICAC (SA) | 10 | 396 | 386 | - |
| NSW CC | 727 | 30,336 | 24,250 | 83 |
| NSW Police | 898 | 31,293 | 19,957 | 21 |
| NT Police | 398 | 10,699 | 8,901 | 1 |
| PIC | 103 | 4,461 | 3,816 | 3 |
| QLD Police | 4,191 | 181,694 | 158,596 | 231 |
| SA Police | 403 | 15,931 | 11,500 | 8 |
| TAS Police | 169 | 7,517 | 5,067 | 14 |
| VIC Police | 6,733 | 133,316 | 96,102 | 142 |
| WA Police | 1,073 | 48,285 | 29,564 | 78 |
| **Total** | **20,105** | **619,558** | **458,438** | **899** |

The table also outlines the number of days the authorisations were to be in force and how many days they were actually in force.

Table 38 compares 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 between 2014–15 and 2015–16.

**Table 38: Average specified and actual time in force of prospective data authorisations**

| Agency | Average period specified | | Average period actual | |
|---|---|---|---|---|
| | 14/15 | 15/16 | 14/15 | 15/16 |
| ACC | 30 | 19 | 19 | 15 |
| ACLEI | 27 | 38 | 17 | 38 |
| AFP | 38 | 38 | 26 | 24 |
| CCC (QLD) | 29 | 26 | 23 | 15 |
| CCC (WA) | 43 | 43 | 23 | 35 |
| DIBP | 1 | 1 | 1 | 1 |
| IBAC | 43 | 42 | 38 | 36 |
| ICAC (NSW) | 29 | 45 | 21 | 23 |
| ICAC (SA) | 41 | 40 | 35 | 39 |
| NSW CC | 39 | 42 | 35 | 38 |
| NSW Police | 35 | 35 | 21 | 23 |
| NT Police | 43 | 27 | 37 | 22 |
| PIC | 42 | 44 | 35 | 38 |
| QLD Police | 43 | 43 | 39 | 40 |
| SA Police | 39 | 40 | 26 | 29 |
| TAS Police | 45 | 44 | 33 | 33 |
| VIC Police | 20 | 20 | 9 | 15 |
| WA Police | 45 | 45 | 36 | 30 |
| **Average** | **35** | **35** | **26** | **27** |

## 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 2015–16, the AFP made 53 data authorisations for access to telecommunications data for the enforcement of the criminal law of a foreign country.

Following these requests, the AFP made 23 disclosures to foreign law enforcement agencies. Information was disclosed to the following countries: Taiwan, Hong Kong, Serbia, Switzerland, Solomon Islands, United Kingdom, New Zealand, Zimbabwe, Argentina, Slovenia, Canada, Germany, Singapore, Indonesia, United States of America, Papua New Guinea, Republic of Ireland, Netherlands, People's Republic of China, Spain and France.

## Further reporting requirements

Tables 39 and 40 set out the offences for which authorised officers of an agency made authorisations for the enforcement of the criminal law, a law imposing a pecuniary penalty, or the protection of the public revenue. The offence categories listed in each table are based on the Australian and New Zealand Standard Offence Classification, published by the Australian Bureau of Statistics. In collaboration with criminal law enforcement agencies that provided data to the department, the department has added additional categories to better reflect the offence categories for which data authorisations may be made.

**Table 39: Offences for which authorisations were made to access existing data to enforce the criminal law between 13 October 2015 and 30 June 2016– s. 186(1)(e)[12]**

| Categories of offences | ACCC | ACC | ACLEI | AFP | ASIC | CCC (QLD) | CCC (WA) | DIBP | IBAC | ICAC (NSW) | ICAC (SA) | NSW CC | NSW Police | NT Police | PIC | QLD Police | SA Police | TAS Police | VIC Police | WA Police | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Abduction | - | - | - | 254 | - | - | - | - | - | - | - | 2 | 3,349 | 67 | - | 935 | 313 | 85 | 2,773 | 2,269 | **10,047** |
| ACC investigation | - | 5,972 | - | 1 | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | **5,973** |
| Acts—injury | - | - | - | 150 | - | - | - | - | - | - | - | - | 2,698 | 40 | 6 | 5 | 154 | 180 | 5,149 | 1,098 | **9,480** |
| Bribery or corruption | - | - | 1,808 | 322 | - | 573 | 367 | - | 22 | 109 | 74 | 2 | 20 | 6 | 786 | - | 826 | - | 141 | 1,090 | **6,146** |
| Cartel offences | 34 | - | - | 10 | - | - | - | - | - | - | - | - | 13 | - | - | - | - | - | - | - | **57** |
| Conspire | - | - | - | 31 | 6 | - | - | - | - | - | - | - | 106 | - | - | - | - | - | 249 | 6 | **398** |
| Cybercrime | - | - | - | 1,472 | - | 143 | 1 | - | - | - | - | - | 1,986 | 18 | 3 | 149 | 23 | 119 | 400 | 168 | **4,482** |
| Dangerous acts | - | - | - | 124 | - | - | - | - | - | - | - | - | 440 | 51 | - | 690 | 240 | - | 2,714 | 100 | **4,359** |
| Fraud | - | - | - | 1,277 | 499 | 90 | - | 413 | 87 | - | 12 | 601 | 5,179 | 82 | - | 481 | 485 | 260 | 953 | 863 | **11,282** |
| Homicide | - | - | - | 559 | - | - | - | - | - | - | - | 358 | 7,127 | 101 | - | 1,661 | 1,695 | 1,318 | 9,435 | 2,991 | **25,245** |
| Illicit drug offences | - | - | - | 9,504 | - | 1,240 | - | 1,226 | 17 | - | - | 545 | 15,189 | 1,089 | 104 | 5,102 | 4,121 | 1,314 | 8,481 | 9,234 | **57,166** |
| Loss of life | - | - | - | 72 | - | - | - | - | - | - | - | - | 291 | 6 | - | 242 | 3 | 17 | 5,511 | 95 | **6,237** |
| Miscellaneous | - | - | - | 306 | 925 | - | - | 19 | - | - | - | - | 2,126 | 104 | 12 | 2,973 | 506 | 36 | 5,359 | 350 | **12,716** |
| Justice procedures | - | - | - | 105 | 14 | - | - | 3 | 25 | - | 1 | - | 315 | 13 | - | - | 38 | 56 | 400 | 358 | **1,328** |
| Organised offences | - | - | - | 327 | - | - | - | - | - | - | - | - | 1,265 | 8 | - | - | 17 | - | 2,271 | 160 | **4,048** |

12 Appendix F contains a description of each of the categories of offences.

| Categories of offences | ACCC | ACC | ACLEI | AFP | ASIC | CCC (QLD) | CCC (WA) | DIBP | IBAC | ICAC (NSW) | ICAC (SA) | NSW CC | NSW Police | NT Police | PIC | QLD Police | SA Police | TAS Police | VIC Police | WA Police | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Pecuniary penalty | - | - | - | 70 | - | - | - | - | - | - | - | - | 253 | 2 | - | - | - | 39 | - | 43 | **407** |
| Public revenue | - | - | - | 68 | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | 17 | **85** |
| People smuggling | - | - | - | 147 | - | - | - | 4 | - | - | - | - | 1 | 1 | - | - | - | - | - | - | **153** |
| Weapons | - | - | - | 133 | - | - | - | 75 | - | - | - | 1 | 1,350 | 1 | - | 12 | 32 | 5 | 5,234 | 21 | **6,864** |
| Property damage | - | - | - | 31 | - | - | - | - | - | - | - | - | 879 | 2 | - | - | 256 | - | 3,686 | 102 | **4,956** |
| Public order offences | - | - | - | 84 | - | - | - | - | - | - | - | - | 45 | - | - | 22 | 1 | - | - | 29 | **181** |
| Robbery | - | - | - | 215 | - | - | - | - | - | - | - | 2 | 6,137 | 94 | - | 624 | 297 | 83 | 3,259 | 1,084 | **11,795** |
| Serious damage | - | - | - | 31 | - | - | - | - | - | - | - | 11 | 460 | - | - | 335 | 29 | 214 | 1,015 | 193 | **2,288** |
| Sexual assault | - | - | - | 377 | - | - | - | 9 | - | - | - | 1 | 3,851 | 83 | - | 730 | 686 | 586 | 1,771 | 1,303 | **9,397** |
| Terrorism offences | - | - | - | 1,764 | - | - | - | 15 | - | - | - | 171 | 1,015 | 2 | - | 1 | 10 | - | 340 | 1,136 | **4,454** |
| Theft | - | - | - | 738 | - | - | 38 | 5 | - | - | - | 1 | 3,248 | 86 | 3 | 763 | 301 | 794 | 3,297 | 1,073 | **10,347** |
| Traffic | - | - | - | 16 | - | - | - | - | - | - | - | - | 402 | 6 | - | 128 | 12 | - | 150 | 49 | **763** |
| Unlawful entry | - | - | - | 27 | - | - | - | - | - | - | - | - | 1,393 | 55 | - | 1,233 | 161 | 608 | 3,986 | 2,058 | **9,521** |
| **Total** | **34** | **5,972** | **1,808** | **18,215** | **1,444** | **2,046** | **406** | **1,769** | **151** | **109** | **87** | **1,695** | **59,138** | **1,917** | **914** | **16,086** | **10,206** | **5,714** | **66,574** | **25,890** | **220,175** |

**Table 40: Offences against which authorisations were made for access to existing information or documents in enforcement of a pecuniary penalty or protection of the public revenue for the period 13 October 2015 to 30 June 2016—s. 186(1)(e)13**

| Categories of offences | ACCC | AFP | ASIC | DIBP | IBAC | NSW Police | NT Police | QLD Police | SA Police | TAS Police | WA Police | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Abduction | - | - | 2 | - | - | 44 | - | - | - | - | - | **46** |
| Acts - injury | - | - | - | - | - | 21 | - | - | - | 30 | - | **51** |
| Bribery or corruption | - | 1 | - | - | - | - | - | - | - | - | - | **1** |
| Cybercrime | - | - | - | - | - | 9 | - | - | - | 19 | - | **28** |
| Dangerous acts | - | - | - | - | - | 4 | - | - | - | - | 13 | **17** |
| Fraud | 10 | 8 | 90 | 10 | 1 | 33 | - | - | - | - | 2 | **154** |
| Homicide | - | - | - | - | - | 41 | - | 2 | - | - | 8 | **51** |
| Illicit drug offences | - | 2 | - | 15 | - | 291 | - | 1 | - | - | - | **309** |
| Loss of life | - | - | - | - | - | 8 | - | 1 | - | - | 1 | **10** |
| Miscellaneous | - | - | 8 | - | - | 31 | 2 | 1 | - | 7 | 8 | **57** |
| Justice procedures | - | 1 | 5 | - | - | 2 | - | - | - | 49 | - | **57** |
| Organised offences | - | - | - | - | - | 5 | - | - | - | - | - | **5** |
| Pecuniary penalty | - | 11 | - | 11 | - | 115 | - | - | 1 | 373 | - | **511** |
| Public revenue | - | 12 | - | - | - | - | - | - | - | - | - | **12** |
| Weapons | - | 2 | - | 7 | - | 35 | - | - | - | 28 | - | **72** |
| Robbery | - | - | 2 | - | - | 43 | - | - | - | 2 | - | **47** |
| Serious damage | - | - | - | - | - | 3 | - | - | - | - | - | **3** |

13 Appendix F contains a description of each of the categories of offences.

| Categories of offences | ACCC | AFP | ASIC | DIBP | IBAC | NSW Police | NT Police | QLD Police | SA Police | TAS Police | WA Police | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Sexual assault | - | - | - | - | - | 21 | - | - | - | - | 2 | **23** |
| Terrorism offences | - | - | - | - | - | 1 | - | - | - | - | - | **1** |
| Theft | - | - | - | - | - | 41 | - | 1 | - | 113 | - | **155** |
| Traffic | - | - | - | - | - | 26 | - | - | - | 44 | 20 | **90** |
| Unlawful entry | - | - | - | - | - | 17 | - | 1 | - | - | - | **18** |
| **Total** | **10** | **37** | **107** | **43** | **1** | **791** | **2** | **7** | **1** | **665** | **54** | **1,718** |

**Table 41: Offences against which authorisations were made for access to specified information or documents that come into existence during the period for which an authorisation is in force for the period 13 October 2015 to 30 June 2016—s. 186(1)(e)[14]**

| Categories of offences | ACC | ACLEI | AFP | CCC (QLD) | CCC (WA) | DIBP | IBAC | ICAC (NSW) | ICAC (SA) | NSW CC | NSW Police | NT Police | PIC | QLD Police | SA Police | TAS Police | VIC Police | WA Police | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Abduction | - | - | 17 | - | - | - | - | - | - | 2 | 23 | 2 | - | 21 | 19 | 9 | 669 | 14 | **776** |
| ACC investigation | 1,578 | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | **1,578** |
| Acts - injury | - | - | 7 | - | - | - | - | - | - | - | 41 | 4 | - | 70 | 7 | - | 68 | 29 | **226** |
| Bribery or corruption | - | 67 | 17 | 8 | 32 | - | 6 | 1 | 5 | - | - | - | 44 | - | - | - | 23 | 1 | **204** |
| Conspire | - | - | 1 | - | - | - | - | - | - | - | 10 | - | - | 1 | - | - | 2 | - | **14** |
| Cybercrime | - | - | 38 | 3 | 1 | - | - | - | - | - | - | - | - | 4 | - | - | 4 | - | **50** |
| Dangerous acts | - | - | 3 | - | - | - | - | - | - | - | 5 | - | - | - | 4 | - | 799 | 11 | **822** |
| Fraud | - | - | 174 | 1 | - | 34 | 28 | - | - | 195 | 35 | 1 | - | 29 | 1 | 4 | 37 | 23 | **562** |
| Homicide | - | - | 11 | - | - | - | - | - | - | 39 | 37 | 1 | - | 174 | 6 | 4 | 727 | 33 | **1,032** |
| Illicit drug offences | - | - | 1,286 | 88 | - | 48 | 10 | - | - | 158 | 302 | 223 | 4 | 2,066 | 196 | 72 | 607 | 426 | **5,486** |
| Loss of life | - | - | 1 | - | - | - | - | - | - | - | 7 | - | - | 2 | - | - | 169 | - | **179** |
| Miscellaneous | - | - | 41 | - | - | 1 | - | - | - | - | 17 | - | - | 11 | 11 | 5 | 200 | 11 | **297** |
| Justice procedures | - | - | 2 | - | - | - | 26 | - | - | - | 4 | - | - | - | - | - | 5 | - | **37** |
| Organised offences | - | - | 57 | - | - | - | - | - | - | - | 27 | - | - | - | 3 | - | 223 | - | **310** |
| People smuggling | - | - | 7 | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | **7** |
| Weapons | - | - | 40 | - | - | 8 | - | - | - | - | 49 | - | - | 14 | 3 | 1 | 67 | 7 | **189** |
| Property damage | - | - | - | - | - | - | - | - | - | - | 3 | - | - | 1 | 2 | - | 22 | - | **28** |
| Public order offences | - | - | - | - | - | - | - | - | - | - | 2 | - | - | 1 | - | - | - | - | **3** |

14 Appendix F contains a description of each of the categories of offences.

| Categories of offences | ACC | ACLEI | AFP | CCC (QLD) | CCC (WA) | DIBP | IBAC | ICAC (NSW) | ICAC (SA) | NSW CC | NSW Police | NT Police | PIC | QLD Police | SA Police | TAS Police | VIC Police | WA Police | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Robbery | - | - | - | - | - | - | - | - | - | 1 | 88 | 2 | - | 82 | 8 | - | 373 | 32 | **586** |
| Serious damage | - | - | - | - | - | - | - | - | - | - | 3 | - | - | 6 | - | - | 116 | 5 | **130** |
| Sexual assault | - | - | 14 | - | - | - | - | - | - | - | 7 | 3 | - | 12 | 2 | 1 | 557 | 7 | **603** |
| Terrorism offences | - | - | 150 | - | - | 1 | - | - | - | 126 | 2 | - | - | - | 1 | - | 126 | 10 | **416** |
| Theft | - | - | 63 | - | 4 | 1 | - | - | - | - | 27 | - | - | 34 | 6 | 2 | 344 | 27 | **508** |
| Traffic | - | - | - | - | - | - | - | - | - | - | - | - | - | 4 | - | - | 4 | - | **8** |
| Unlawful entry | - | - | 1 | - | - | - | - | - | - | - | 11 | 2 | - | 121 | 14 | 15 | 338 | 114 | **616** |
| **Total** | **1,578** | **67** | **1,930** | **100** | **37** | **93** | **70** | **1** | **5** | **521** | **700** | **238** | **48** | **2,653** | **283** | **113** | **5,480** | **750** | **14,667** |

Table 42 lists the length of time for which information or documents covered by historical data authorisations had been held by a telecommunications carrier before the authorisations for that information was made. The statistics are spilt into successive periods of 3 months and include the total number of authorisations made for data held for the lengths of time specified. The information covers the mandatory retention period for telecommunications data and provides an indication of how frequently data is accessed over two years.

For the period from 13 October 2015 to 30 June 2016 83 per cent of authorisations were for data 0–3 months old. Authorisations for 'point in time' information without an identifiable age, such as current subscriber information and current information held in the Integrated Public Number Database,[15] have been recorded as '0' months old and are included in the 0–3 month field.

Subscriber information and other customer identification information constitute the majority of authorisations included in the 0-3 month bracket. This type of information is commonly used at the beginning of an investigation to identify and eliminate suspects. During the period 13 October 2015 to 30 June 2016 a significant number of authorisations for identifying information related to current subscriber checks or other information without an identifiable age.

15 The Integrated Public Number Database is an industry-wide database, managed by Telstra, containing all listed and unlisted public telephone numbers.

**Table 42: Periods which retained data was held by carrier before authorised disclosure for the period 13 October 2015 to 30 June 2016—s. 186(1)(f)**

| Agency | Age of data under disclosure | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | 0–3 mths | 3–6 mths | 6–9 mths | 9–12 mths | 12–15 mths | 15–18 mths | 18–21 mths | 21–24 mths | Over 24 mths | **Total** |
| ACCC | - | 3 | 2 | - | 1 | 13 | 6 | 6 | 13 | **44** |
| ACC | 5,727 | 112 | 42 | 59 | 7 | 8 | 2 | 4 | 11 | **5,972** |
| ACLEI | 1,793 | 3 | 2 | 2 | 3 | - | - | 5 | - | **1,808** |
| AFP | 12,148 | 2,499 | 821 | 1,101 | 470 | 202 | 96 | 172 | 752 | **18,261** |
| ASIC | 1,189 | 64 | 27 | 16 | 6 | 11 | 20 | 14 | 36 | **1,383** |
| CCC (QLD) | 1,219 | 430 | 97 | 121 | 70 | 35 | - | - | 74 | **2,046** |
| CCC (WA) | 406 | 4 | - | - | - | - | - | - | - | **410** |
| DIBP | 457 | 201 | 86 | 68 | 37 | 14 | 7 | 9 | 1,026 | **1,905** |
| IBAC | 112 | 22 | 5 | 3 | 2 | - | 1 | - | 7 | **152** |
| ICAC (NSW) | 32 | 23 | 10 | 9 | 6 | 8 | 1 | 1 | 18 | **108** |
| ICAC (SA) | 14 | 7 | 12 | 16 | 2 | - | 14 | 1 | 7 | **73** |
| NSW CC | 1,296 | 87 | 33 | 28 | 33 | 13 | 20 | 29 | 156 | **1,695** |
| NSW Police | 66,900 | 3,398 | 1,040 | 1,152 | 516 | 294 | 190 | 249 | 806 | **74,545** |
| NT Police | 1,708 | 64 | 26 | 18 | 13 | 18 | 6 | 6 | 25 | **1,884** |
| PIC | 625 | 68 | 67 | 16 | 18 | 1 | 9 | 17 | 74 | **895** |
| QLD Police | 13,195 | 1,177 | 737 | 335 | 264 | 121 | 76 | 73 | 371 | **16,349** |
| SA Police | 5,931 | 1,322 | 310 | 714 | 448 | 55 | 21 | 41 | 645 | **9,487** |
| TAS Police | 5,746 | 233 | 78 | 48 | 5 | 2 | - | 10 | 387 | **6,509** |
| VIC Police | 53,425 | 5,381 | 3,351 | 2,131 | 1,387 | 1,257 | 685 | 27 | 11 | **67,655** |
| WA Police | 24,723 | 486 | 205 | 151 | 111 | 54 | 35 | 45 | 80 | **25,890** |
| **Total** | **196,646** | **15,584** | **6,951** | **5,988** | **3,399** | **2,106** | **1,189** | **709** | **4,499** | **237,071** |

Table 43 lists the number of occasions from 13 October 2015 to 30 June 2016 that agencies made authorisations for retained data which included information from the data subsets identified in subsection 187AA(1). Data within item 1 of that subsection is typically considered 'subscriber data' and includes information identifying the user of a telecommunications service. Data within items 2-6 of that subsection are typically considered 'traffic data' and include information such as the time, duration and source of a communication.[16]

**Table 43: Types of retained data disclosed in authorisations for the period 13 October 2015 to 30 June 2016—ss. 186(1)(g) and 186(1)(h)**

| Agency | Number of authorisations which included information from the data sets identified in subsection 187AA(1) | | |
|---|---|---|---|
| | Item 1: subscriber data | Items 2–6: traffic data | **Total** |
| ACCC | 33 | 11 | **44** |
| ACC | 3,676 | 2,296 | **5,972** |
| ACLEI | 1,773 | 35 | **1,808** |
| AFP | 12,599 | 5,662 | **18,261** |
| ASIC | 1,096 | 287 | **1,383** |
| CCC (QLD) | 1,706 | 340 | **2,046** |
| CCC (WA) | 377 | 37 | **414** |
| DIBP | 1,524 | 381 | **1,905** |
| IBAC | 96 | 71 | **167** |
| ICAC (NSW) | 35 | 75 | **110** |
| ICAC (SA) | 25 | 48 | **73** |
| NSW CC | 1,197 | 702 | **1,899** |
| NSW Police | 52,684 | 21,861 | **74,545** |
| NT Police | 1,351 | 532 | **1,883** |
| PIC | 686 | 893 | **1,579** |
| QLD Police | 12,407 | 5,991 | **18,398** |
| SA Police | 8,882 | 2,235 | **11,117** |
| TAS Police | 5,382 | 1,127 | **6,509** |
| VIC Police | 43,414 | 24,241 | **67,655** |
| WA Police | 21,059 | 4,831 | **25,890** |
| **Total** | **170,002** | **71,656** | **241,658** |

16 Appendix E further explains the type of data included in items 1-6 of the table at 187AA(1).

## Journalist information warrants

The Data Retention Act established the journalist information warrant (JIW) scheme. This scheme requires enforcement agencies to obtain a warrant prior to authorising the disclosure of telecommunications data to identify a journalist's source. Enforcement agencies are prohibited from making data authorisations for access to a journalist's or their employer's data for the purpose of identifying a confidential source unless a JIW is in force.

For the period between 13 October 2015 to 30 June 2016, 33 authorisations were made under two JIWs issued to the WA Police. These authorisations were for the purpose of enforcing the criminal law.

## Industry estimated cost of implementing data retention obligations

Information collected from industry through the Data Retention Industry Grants Programme, indicates that the estimated capital cost of implementing data retention obligations over the period between 30 October 2014 and 13 April 2017 is $198,527,354.

Costs that service providers detailed as part of their grant applications were incurred between 30 October 2014-13 April 2017 and relate to the anticipated direct up-front capital costs and not the recurring or indirect costs associated with compliance. Table 44 represents the baseline figure indicating the reportable anticipated capital cost to industry representatives that applied for a grant, broken down by financial year.

**Table 44: Industry Capital Costs of data retention—s. 187P(1A)**

| | Anticipated costs |
|---|---|
| 2014–15 | 3,819,642 |
| 2015–16 | 68,977,652 |
| 2016–17 | 125,730,060 |
| **Total** | **198,527,354** |

The total funding made available under the Data Retention Industry Grants Programme was $128,351,400. 210 applications were received of which 10 later withdrew. A total of 180 providers were found eligible for funding, with most awarded a grant representative of 80 per cent of their anticipated costs of compliance.

## Use of data retention plans

The Data Retention Act came into effect on 13 October 2015 and providers were able to apply to the Communications Access Co-ordinator for an additional 18 months to comply with the legislation through an approved Data Retention Implementation Plan. During the 18 month implementation period which ended on 13 April 2017, the Attorney-General's Department received 402 Data Retention Implementation Plans from 310 providers. The plans were assessed by the Communications Access Co-ordinator in accordance with the process in section 187F of the Act, including consultation with agencies and the Australian Communications Media Authority under section 187G.

# CHAPTER 4

## FURTHER INFORMATION

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

Communications Security and Intelligence Branch
Attorney-General's Department
3-5 National Circuit
BARTON ACT 2600

(02) 6141 2900

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

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

# APPENDIX A

## LIST OF TABLES AND FIGURES

### Tables

## Figures

# APPENDIX B

## INTERCEPTION AGENCIES UNDER THE TIA ACT

| Commonwealth agency or state eligible authority | Date of s.34 declaration |
|---|---|
| Australian Commission for Law Enforcement Integrity | Not applicable |
| Australian Crime Commission | Not applicable |
| Australian Federal Police | Not applicable |
| Corruption and Crime Commission (Western Australia) | 26 March 2004 |
| Crime and Corruption Commission (Queensland) | 7 July 2009 |
| Independent Broad-based Anti-corruption Commission (Victoria) | 18 December 2012 (came into force 10 February 2013) |
| Independent Commission Against Corruption (New South Wales) | 6 June 1990 |
| New South Wales Crime Commission | 30 January 1989 |
| New South Wales Police Force | 30 January 1989 |
| Northern Territory Police | 25 October 2006 |
| Police Integrity Commission (New South Wales) | 14 July 1998 |
| Queensland Police Service | 8 July 2009 |
| Independent Commissioner Against Corruption (South Australia) | 17 June 2013 (came into force 1 September 2013) |
| South Australia Police | 10 July 1991 |
| Tasmania Police | 5 February 2005 |
| Victoria Police | 28 October 1988 |
| Western Australia Police | 15 July 1997 |

# APPENDIX C

## ABBREVIATIONS

| ACRONYM | AGENCY / ORGANISATION |
|---|---|
| AAT | Administrative Appeals Tribunal |
| ACC | Australian Crime Commission[17] |
| 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) |
| DIBP | Department of Immigration and Border Protection (including the Australian Customs and Border Protection Service) |
| Defence (IGD, ADFIS) | Inspector-General Defence, Australian Defence Force Investigative Service |
| 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 |
| 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) |

17 The merge of CrimTrac and the Australian Crime Commission (ACC) took effect on 1 July 2016, ACIC will be used in future annual reports to represent the former ACC.

| ACRONYM | AGENCY / ORGANISATION |
|---|---|
| SA Police | South Australia Police |
| TAS Police | Tasmania Police |
| Telecommunications Act | *Telecommunications Act 1997* |
| TIA Act | *Telecommunications (Interception and Access) Act 1979* |
| VIC Police | Victoria Police |
| WA Police | Western Australia Police |

# APPENDIX D

## CATEGORIES OF SERIOUS OFFENCES

| Serious offence category | Offences covered |
|---|---|
| ACC special investigation | TIA Act, s5D(1)(f) |
| 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) |
| 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),; 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) |
| Child pornography offences | TIA Act, s5D(3B) |
| Conspire / aid / abet serious offence | TIA Act, s5D(6) |
| Cybercrime offences | TIA Act, s5D(5) |
| Kidnapping | TIA Act, s5D(1)(b) |
| Loss of life or personal injury | TIA Act, s5D(2)(b)(i) and (ii) |
| Money laundering | TIA Act, s5D(4) |
| Murder | TIA Act, s5D(1)(a) |
| Organised offences and/or criminal organisations | TIA Act, s5D(3; s5D(8A) and (9) |
| People smuggling and related | TIA Act, s5D(3A) |
| Serious damage to property and/or serious arson | TIA Act, s5D(2)(b)(iii) and (iiia) |
| Serious drug offences and/or trafficking | TIA Act, s5D(5A); s5D(2)(b)(iv); TIA Act, s5D(1)(c) |
| Serious fraud and/or revenue loss | TIA Act, s5D(2)(v) and (vi) |
| Telecommunications offences | TIA Act, s5D(5)(a) |
| Terrorism offences | TIA Act, s5D(1)(d), 5D(1)(e) |

# APPENDIX E

## RETAINED DATA SETS

| Item | Description of information | Explanation |
|---|---|---|
| 1. The subscriber of, and accounts, services, telecommunications devices and other relevant services relating to, the relevant service | The following:<br>(a) any information that is one or both of the following:<br>i) any name or address information;<br>ii) any other information for identification purposes;<br>relating to the relevant service, being information used by the service provider for the purposes of identifying the subscriber of the relevant service;<br>(b) any information relating to any contract, agreement or arrangement relating to the relevant account, service or device;<br>(c) any information that is one or both of the following:<br>i) billing or payment information;<br>ii) contact information;<br>relating to the relevant service, being information used by the service provider in relation to the relevant service;<br>(d) any identifiers relating to the relevant service or any related account, service or device, being information used by the service provider in relation to the relevant service or any related account, service or device;<br>(e) the status of the relevant service or any related account, service or device | This category includes customer identifying details, such as name and address. It also includes contact details, such as phone number and email address. This information allows agencies to confirm a subscriber's identity or link a service or account to a subscriber.<br>This category also includes details about services attached to account, such as the unique identifying number attached to a mobile phone, or the IP address (or addresses) allocated to an internet access account or service.<br>This category further includes billing and payment information.<br>Information about the status of a service can include when an account has been enabled or suspended, a relevant service has been enabled or suspended or is currently roaming, or a telecommunications device has been stolen.<br>The phrases 'any information' and 'any identifiers' should be read to mean the information that the provider obtains or generates that meets the description which follows that phrase. If the provider has no information that meets the description, including because that kind of information does not pertain to the service in question, no information needs to be retained. |

*Continued next page*

| Item | Description of information | Explanation |
|---|---|---|
| | | For instance, if a provider offers a free service and therefore has no billing information, no billing information needs to be retained by that provider with respect to that service the provider will need to retain subscriber and transactional data with respect to that service, but no billing information needs to be retained.<br><br>Service providers are not required to collect and retain passwords, PINs, secret questions or token codes, which are used for authentication purposes. |
| 2. The source of a communication | Identifiers of a related account, service or device from which a communication has been sent or attempted to be sent by means of the relevant service. | Identifiers for the source of a communication may include, but are not limited to:<br>• the phone number, IMSI, IMEI from which a call or SMS was made<br>• identifying details (such as username, address, number) of the account, service or device from which a text, voice, or multi-media communication was made (examples include email, Voice over IP (VoIP), instant message or video communication)<br>• the IP address and port number allocated to the subscriber or device connected to the internet at the time of the communication, or<br>• any other service or device identifier known to the provider that uniquely identifies the source of the communication.<br><br>In all instances, the identifiers retained to identify the source of the communication are the ones relevant to, or used in, the operation of the particular service in question. |

| Item | Description of information | Explanation |
|---|---|---|
| 3. The destination of a communication | Identifiers of the account, telecommunications device or relevant service to which the communication:<br>a) has been sent; or<br>b) has been forwarded, routed or transferred, or attempted to be forwarded, routed or transferred. | Paragraph 187A(4)(b) puts beyond doubt that service providers are not required to keep information about subscribers' web browsing history.<br>The destination of a communication is the recipient. Identifiers for the destination of a communication may include, but are not limited to:<br>• the phone number that received a call or SMS<br>• identifying details (such as username, address or number) of the account, service or device which receives a text, voice or multi-media communication (examples include email, VoIP, instant message or video communication)<br>• the IP address allocated to a subscriber or device connected to the internet at the time of receipt of the communication, or<br>• any other service or device identifier known to the provider that uniquely identifies the destination of the communication.<br>For internet access services, the Bill explicitly excludes anything that is web-browsing history or could amount to web-browsing history, such as a URL or IP address to which a subscriber has browsed.<br>In all instances, the identifiers retained to identify the destination of the communications are the ones relevant to, or used in, the operation of the particular service in question. If the ultimate destination of a communication is not feasibly available to the provider of the service, the provider must retain only the last destination knowable to the provider. |

| Item | Description of information | Explanation |
|---|---|---|
| 4. The date, time and duration of a communication, or of its connection to a relevant service | The date and time (including the time zone) of the following relating to the communication (with sufficient accuracy to identify the communication):<br>a) the start of the communication<br>b) the end of the communication<br>c) the connection to the relevant service, and<br>d) the disconnection from the relevant service. | For phone calls this is simply the time a call started and ended.<br>For internet sessions this is when a device or account connects to a data network and ends when it disconnected—those events may be a few hours to several days, weeks, or longer apart, depending on the design and operation of the service in question. |
| 5. The type of a communication and relevant service used in connection with a communication | The following:<br>a) the type of communication;<br>Examples: Voice, SMS, email, chat, forum, social media.<br>b) the type of the relevant service;<br>Examples: ADSL, Wi-Fi, VoIP, cable, GPRS, VoLTE, LTE.<br>c) the features of the relevant service that were, or would have been, used by or enable for the communication.<br>Examples: call waiting, call forwarding, data volume usage. | The type of communication means the form of the communication (for example voice call vs. internet usage).<br>The type of the relevant service (5(b)) provides more technical detail about the service. For example, for a mobile messaging service, whether it is an SMS or MMS.<br>Data volume usage, applicable to internet access services, refers to the amount of data uploaded and downloaded by the subscriber. This information can be measured for each session, or in a way applicable to the operation and billing of the service in question, such as per day or per month.<br>Note: This item will only apply to the service provider operating the relevant service: see paragraph 187A(4)(c). |

| Item | Description of information | Explanation |
|---|---|---|
| 6. The location of equipment or a line used in connection with a communication | The following in relation to the equipment or line used to send or receive the communication:<br>a) the location of the equipment or line at the start of the communication;<br>b) the location of the equipment or line at the end of the communication.<br>Examples: Cell towers, Wi-Fi hotspots. | Location records are limited to the location of a device at the start and end of a communication, such as a phone call or Short Message Service (SMS) message.<br>For services provided to a fixed location, such as an ADSL service, this requirement can be met with the retention of the subscriber's address.<br>Paragraph 187A(4)(e) of the Bill provides that location records are limited to information that is used by a service provider in relation to the relevant service. This would include information such as which cell tower, Wi-Fi hotspot or base station a device was connected to at the start and end of communication.<br>Service providers are not required to keep continuous, real-time or precise location records, such as the continuous GPS location of a device. These limitations seek to ensure that the locations records to be kept by service providers do not allow continuous monitoring or tracking of devices. |

# APPENDIX F

## CATEGORIES OF OFFENCES ABBREVIATIONS

| ABBREVIATION | OFFENCE CATEGORY |
|---|---|
| Abduction | Abduction, harassment and other offences against the person |
| Acts - injury | Acts intended to cause injury |
| Conspire | Conspire/aid/abet serious offences |
| Cybercrime | Cybercrime and telecommunications offences |
| Dangerous acts | Dangerous or negligent acts and endangering a person |
| Fraud | Fraud, deception and related offences |
| Homicide | Homicide and related offences |
| Miscellaneous | Miscellaneous offences |
| Justice procedures | Offences against justice procedures, government security and government operations |
| Organised offences | Organised offences and/or criminal organisations |
| Pecuniary penalty | Other offences relating to the enforcement of a law imposing a pecuniary penalty |
| Public revenue | Other offences relating to the enforcement of a law protecting the public revenue |
| People smuggling | People smuggling and related |
| Weapons | Prohibited and regulated weapons and explosive offences |
| Property damage | Property damage and environment pollution |
| Robbery | Robbery, extortion and related offences |
| Serious damage | Serious damage to property |
| Sexual assault | Sexual assault and related offences |
| Theft | Theft and related offences |
| Traffic | Traffic and vehicle regulatory offences |
| Unlawful entry | Unlawful entry with intent/burglary, break and enter |