Australian Government

Department of Home Affairs

Telecommunications (Interception and Access) Act 1979

Annual Report 2018–19

ISSN: 1833-4490 (Print)
ISSN: 2652-1660 (Online)

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

National Security Policy Branch
Department of Home Affairs
PO Box 25
BELCONNEN ACT 2616

Telecommunications (Interception and Access) Act 1979

Annual Report 2018–19

Contents

EXECUTIVE SUMMARY

The *Telecommunications (Interception and Access) Act 1979 Annual Report 2018–19* 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* (the TIA Act) between 1 July 2018 – 30 June 2019.

For the first time, the TIA Act Annual Report for 2018–19 also sets out the extent and circumstances in which eligible Commonwealth, State and Territory government agencies have used the powers available under Part 15 of the *Telecommunications Act 1997* (the Telecommunications Act) to request technical assistance from designated communications providers during the reporting period.

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 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 and authorisations related to these powers is independently overseen by the Commonwealth Ombudsman and equivalent state bodies.

Legislative reforms

Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018

The *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (the Assistance and Access Act) amended several pieces of legislation including the TIA Act (but most notably the Telecommunications Act, through the introduction of Part 15) to establish a modern framework through which Australian law enforcement and national security agencies and the communications industry can work together to address technological obstacles to investigations into serious crimes and national security threats.

The TIA Act Annual Report must now include information about use of the industry assistance framework contained in Part 15 of the Telecommunications Act, as introduced by Schedule 1 of the Assistance and Access Act. This information and further details on the industry assistance framework can be found in chapter four of this report.

Amendments to the TIA Act

Schedule 1 of the Assistance and Access Act also amended the TIA Act to allow the Commonwealth Ombudsman to inspect the records of technical assistance requests, technical assistance notices and technical capability notices given under Part 15 of the Telecommunications Act when the measures have been used in connection with an interception warrant, a stored communications warrant or a telecommunications data authorisation. As the new industry assistance measures complement these existing TIA Act powers, this ensures the Commonwealth Ombudsman can oversee their joint use.

Schedule 2 of the Assistance and Access Act amended the TIA Act to permit ASIO or a law enforcement agency to undertake limited interception in order to execute a computer access warrant. For technical reasons, it may be necessary for an agency to intercept communications for the purposes of executing a computer access warrant. Section 27E(2)(h) of the *Surveillance Devices Act 2004* (SD Act) and section 27E(2)(ea) of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) permit intercepting a communication passing over a telecommunications system if the interception is for the purposes of doing anything specified in a computer access warrant. Intercepted information obtained under computer access warrants is subject to the record keeping obligations of the SD Act or the ASIO Act. Law enforcement agencies' use of computer access warrants is reported on separately in the annual report on the SD Act, commencing from the 2018–19 report.[1]

Schedule 2 also amended the TIA Act to permit the head of a security authority such as ASIO to ask the Attorney-General to authorise the security authority to work with a carrier in order to test or develop interception technologies. Previously, the TIA Act only allowed testing by employees of a security authority. The amendments allow carriers to work with security authorities under authorisation, reflecting the practical operation of interception capabilities.

Unexplained Wealth Legislation Amendment Act 2018

The *Unexplained Wealth Legislation Amendment Act 2018* amended the TIA Act to improve information sharing between jurisdictions by allowing Commonwealth, 'participating States', Northern Territory and Australian Capital Territory law enforcement to use, communicate and record lawfully intercepted information in relation to unexplained wealth investigations and proceedings.

The TIA Act already allowed lawfully intercepted information to be used for proceedings for the confiscation or forfeiture of property or for the imposition of a pecuniary penalty in connection with the commission of a prescribed offence, which includes some unexplained wealth proceedings. However, the new provisions ensure that it is available for use in relation to all Commonwealth, and 'participating State' and Territory unexplained wealth matters, including those that do not require a connection with the commission of an offence.

The *Unexplained Wealth Legislation Amendment Act 2018* also made amendments that allow the New South Wales Crime Commission to use, communicate and record lawfully intercepted information in relation to proceedings for the confiscation or

[1] Available on the website of the Department of Home Affairs, at www.homeaffairs.gov.au.

forfeiture of property or the imposition of a pecuniary penalty, in connection with a prescribed offence. These amendments ensure that the Commission can disclose lawfully intercepted information to defendants in proceeds matters without first filing this information as evidence in court, which will assist the Commission in settling proceeds matters out of court.

Policy developments

There were four reviews relating to the Assistance and Access Act and one review relating to the TIA Act that either commenced or were completed in 2018–19.

Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018

The Parliamentary Joint Committee on Intelligence and Security (PJCIS) completed a review of the Telecommunication and Other Legislation Amendment (Assistance and Access) Bill 2018 in December 2018. The Bill was introduced into the House of Representatives by the Minister for Home Affairs on 20 September 2018 and referred to the PJCIS by the Attorney-General for inquiry and report. The review made fifteen recommendations which were accepted by the Government and implemented through amendments to the Bill before passage.

Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018

The PJCIS conducted a review of the Assistance and Access Act following its passage through Parliament. The review considered all aspects of the Assistance and Access Act and its implementation, including a review of Government amendments introduced and passed on 6 December 2018, as referred by the Senate in a second reading amendment on that day. The review was completed in April 2019 and made three recommendations. The Government supported and is implementing these recommendations.

Review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018

The PJCIS is conducting a third review of the Assistance and Access Act and is due to conclude this review by 30 September 2020.[2] This review will build on the findings of the review currently being conducted by the Independent National Security Legislation Monitor and two previous PJCIS reviews.

[2] The *Telecommunications (Interception and Access) Amendment (Assistance and Access Amendments Review) Act 2019* passed the Parliament on 5 December 2019 and deferred the date for the PJCIS to conclude its review from 13 April 2020 to 30 September 2020. This implemented a request from the PJCIS.

Independent National Security Legislation Monitor Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018

The PJCIS on 27 March 2019 referred the Assistance and Access Act for review to the Independent National Security Legislation Monitor (INSLM). The PJCIS has requested the INSLM consider whether the Assistance and Access Act achieves an appropriate balance and whether it contains sufficient safeguards for protecting the rights of individuals and remains proportionate and necessary. The INSLM is due to report by 30 June 2020.

Review of the mandatory data retention regime

The PJCIS on 2 April 2019 began a review of the mandatory retention regime as required by section 187N of the TIA Act. The mandatory data retention regime is a legislative framework at Part 5-1 of the TIA Act which requires carriers, carriage service providers and internet service providers to retain a defined set of telecommunications data for two years, ensuring that such data remains available for law enforcement and national security investigations.

The PJCIS will consider the ongoing effectiveness of the scheme, taking into account changes in the use of technology since it was introduced. It will also reassess the appropriateness of the dataset and the retention period, security requirements in relation to data stored under the regime, and oversight of the regime. The committee is required to report by 13 April 2020.

For further information on these reviews including committee reports and submissions, visit:

- <www.aph.gov.au>
- <www.inslm.gov.au>

Key findings

The following key statistics are relevant to the 2018–19 reporting period.

- 3,561 interception warrants were issued to interception agencies. This was an increase of 37 on the 3,524 issued in 2017–18.
- The majority of serious offences that were specified in interception warrants issued were serious drug and trafficking offences (1,937 times specified), followed by loss of life or personal injury offences (565 times specified) and murder (333 times specified).
- Information obtained under interception warrants was used in:[3]
    - 2,588 arrests;
    - 5,030 prosecutions; and
    - 3,400 convictions.
- 1,252 stored communications warrants were issued to criminal law-enforcement agencies, an increase of 424 on the 828 issued in 2017–18.
- Law enforcement agencies made 565 arrests, conducted 884 proceedings, and obtained 280 convictions based on evidence obtained under stored communications warrants.
- 20 enforcement agencies made 295,691 authorisations for the disclosure of historical telecommunications data – a decrease of 5,433 authorisations from the 301,124 authorisations made in 2017–18. Of these, 291,353 were made to enforce the criminal law.
- The majority of criminal law offences for which historical telecommunications data was requested were illicit drug offences (72,677 requests), followed by 28,457 requests for fraud and related offences and 25,608 requests for homicide offences.
- 27,824 authorisations were made by criminal law-enforcement agencies for the disclosure of prospective telecommunications data, an increase of 3,877 on the 23,947 authorisations made in 2017–18.
- Six journalist information warrants were issued to the AFP under which 20 historical data authorisations were made for the enforcement of the criminal law.
- Two agencies used powers under Part 15 of the *Telecommunications Act 1997* to request technical assistance from designated communications providers. Five technical assistance requests were given by the AFP, and two were given by NSW Police.

[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.

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, or 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

Another 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.

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 and for the location of a missing person.

During the 2018–19 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 *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015*, passed by the Parliament in March 2015, reduced the number of enforcement agencies that may access telecommunications data under the TIA Act to 20 specified agencies. The Minister may declare additional agencies in limited

[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 – but **not** the content of the communication.
[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.

circumstances for a period of 40 sitting days of Parliament. No additional agencies were declared in the 2018–19 reporting period.

Format of Annual Report

The Annual Report is organised into four main chapters:

- Chapter 1 – telecommunications interception;
- Chapter 2 – stored communications;
- Chapter 3 – telecommunications data;
- Chapter 4 – industry technical assistance.

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

More information

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

- Department of Home Affairs <www.homeaffairs.gov.au>
- 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>

CHAPTER 1 – TELECOMMUNICATIONS INTERCEPTION

The primary function of chapter two of the TIA Act, regarding telecommunications interception, 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. The TIA Act prohibits communications from being intercepted while they are passing over an Australian telecommunications system, except as authorised under the circumstances set out in the TIA Act.

Definition

The term **'interception agency'** is defined in section 5 of the TIA Act. An interception agency is limited to bodies such as the AFP 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 warrant that 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 including:

- ACIC, ACLEI and the AFP;
- State and Territory Police; and
- State Anti-Corruption Agencies.

A full list of the agencies able to obtain an interception warrant is provided at Appendix B.

Definition

Section 6 of the TIA Act provides that **interception** of a communication passing over a telecommunications system consists of listening to or recording, by any means, such a communication in its passage over that telecommunications system without the knowledge of the person making the communication.

Serious offences

Interception warrants can only be obtained to investigate serious offences as set out in section 5D of the TIA Act. Serious offences generally carry a penalty of at least seven years' imprisonment.[7]

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

Sections 100(1)(f)-(g) and 100(2)(f)-(g) of the TIA Act provide that this report must list the categories of serious offences specified in interception warrants issued during the year and in relation to those categories, how many serious offences in that category were so specified.

This information is presented in Table 1. This table illustrates the important role telecommunications interception plays in investigating serious crimes. Consistent with previous years, in 2018–19 the majority of warrants obtained were to assist with investigations into serious drug offences (1,937 warrants). Loss of life or personal injury offences were specified in 565 warrants and 333 related to murder investigations. Money laundering was specified as an offence in 202 warrants. The total number of offences is typically larger than the total number of warrants issued, as a warrant 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 with a penalty of less than seven years' imprisonment 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 – sections 100(1)(f), 100(1)(g), 100(2)(f) and 100(2)(g)

Categories of offences	ACIC	ACLEI	AFP	CCC (WA)	IBAC	ICAC (NSW)	ICAC (SA)	LECC	NT Police	NSW CC	NSW Police	QLD CCC	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
ACIC special investigations	50	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**50**
Administration of justice / government offences	-	19	31	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**50**
Assisting person to escape or dispose of proceeds	-	-	-	-	-	-	-	-	-	11	-	-	6	-	-	1	-	**18**
Bribery, corruption and dishonesty offences	-	-	9	14	14	17	10	17	1	-	6	24	-	2	-	3	29	**146**
Cartel offences	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**1**
Child pornography offences	-	-	14	-	-	-	-	-	-	-	1	-	-	-	-	-	-	**15**
Conspire/aid/abet serious offence	16	-	-	-	-	-	9	-	-	-	7	-	1	-	2	1	-	**36**
Cybercrime offences	-	-	11	-	-	-	-	-	-	-	1	-	-	-	-	-	-	**12**
Espionage and foreign interference	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**0**
Kidnapping	-	-	-	-	-	-	-	-	-	-	34	-	-	-	-	3	-	**37**
Loss of life or personal injury	-	-	80	-	3	-	-	-	-	-	368	-	36	2	-	40	36	**565**
Money laundering	41	-	104	-	-	-	-	-	-	34	3	1	-	11	-	-	8	**202**
Murder	-	-	24	-	-	-	-	-	1	1	210	-	29	18	2	32	16	**333**
Offences involving planning and organisation	-	-	9	-	-	-	-	-	-	1	100	-	2	-	2	5	12	**131**

Organised offences and/or criminal organisations	6	-	9	-	-	-	-	-	-	3	17	-	-	-	-	-	-	**35**
People smuggling and related	-	-	11	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**11**
Serious damage to property and/or serious arson	-	-	1	-	-	-	-	-	-	-	40	-	6	6	-	1	5	**59**
Serious drug offences and/or trafficking	87	-	425	-	-	-	-	1	15	85	741	4	202	41	15	74	247	**1,937**
Serious fraud	-	-	51	-	-	2	-	-	-	11	69	-	15	-	1	9	4	**162**
Serious loss of revenue	18	-	37	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**55**
Telecommunications offences	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**0**
Terrorism financing offences	7	-	3	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**10**
Terrorism offences	-	-	117	-	-	-	-	-	-	-	4	-	-	-	-	1	-	**122**
TOTAL	**225**	**19**	**937**	**14**	**17**	**19**	**19**	**18**	**17**	**146**	**1,601**	**29**	**297**	**80**	**22**	**170**	**357**	**3,987**

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.

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
- Federal Circuit Court

Section 103(ab) of the TIA Act provides that this report must contain information about the availability of judges to issue warrants under Part 2-5 and the extent to which nominated AAT members have been used for that purpose.

This information is presented in Tables 2 and 3. In 2018–19 there were 94 issuing authorities for telecommunications interception warrants.

Table 2: Number of Federal Court Judges, Family Court Judges, Federal Circuit Court Judges and nominated AAT members to issue telecommunications interception warrants – section 103(ab)

Issuing Authority	Number eligible
Federal Court judges	15
Family Court judges	8
Federal Circuit Court judges	38
Nominated AAT members	33
TOTAL	**94**

Before issuing an interception warrant the issuing 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.

Issuing of telecommunications interception warrants

Table 3 sets out information stating which authorities issued warrants to each interception agency during 2018–19.

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

Agency	Issuing Authority			
	Family Court judges	Federal Circuit Court judges	Federal Court judges	Nominated AAT members
ACIC	29	16	5	82
ACLEI	-	1	-	10
AFP	5	67	5	557
CCC (WA)	14	-	-	-
IBAC	-	2	-	15
ICAC (NSW)	-	2	1	16
ICAC (SA)	-	7	2	10
LECC	-	-	-	18
NT Police	1	-	16	-
NSW CC	-	-	-	131
NSW Police	-	101	-	1,512
QLD CCC	-	4	-	24
QLD Police	-	270	-	27
SA Police	-	14	18	30
TAS Police	-	-	-	22
VIC Police	-	-	1	169
WA Police	269	-	-	88
TOTAL	**318**	**484**	**48**	**2,711**

Applications for telecommunications interception warrants

Sections 100(1)(a)-(c) and 100(2)(a)-(c) of the TIA Act provide that this report must set out the relevant statistics about applications, telephone applications and renewal applications for interception warrants made by agencies during the year.

Table 4 presents this information. In 2018–19 agencies were issued 3,561 interception warrants, an increase from 2017–18, where 3,524 warrants were issued. 747 renewals of interception warrants were issued in 2018–19.

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

Agency	Relevant Statistics	Applications for warrants		Telephone applications for warrants		Renewal applications	
		17 / 18	18 / 19	17 / 18	18 / 19	17 / 18	18 / 19
ACIC	Made	186	133	-	-	21	14
	Refused	-	1	-	-	-	-
	Issued	186	132	-	-	21	14
ACLEI	Made	16	11	-	-	7	6
	Refused	-	-	-	-	-	-
	Issued	16	11	-	-	7	6
AFP	Made	724	634	2	-	246	201
	Refused	-	-	-	-	-	-
	Issued	724	634	2	-	246	201
CCC (WA)	Made	36	14	-	-	13	-
	Refused	-	-	-	-	-	-
	Issued	36	14	-	-	13	-
IBAC	Made	26	20	-	-	9	3
	Refused	1	3	-	-	1	-
	Issued	25	17	-	-	8	3
ICAC (NSW)	Made	16	19	-	-	7	5
	Refused	-	-	-	-	-	-
	Issued	16	19	-	-	7	5
ICAC (SA)	Made	11	19	-	-	-	4
	Refused	-	-	-	-	-	-
	Issued	11	19	-	-	-	4
LECC	Made	17	18	-	-	5	-
	Refused	-	-	-	-	-	-
	Issued	17	18	-	-	5	-

NT Police	Made	31	18	-	-	-	-
	Refused	1	1	-	-	-	-
	Issued	30	17	-	-	-	-
NSW CC	Made	135	131	-	-	49	25
	Refused	-	-	-	-	-	-
	Issued	135	131	-	-	49	25
NSW Police	Made	1,413	1,613	39	41	309	384
	Refused	3	-	-	-	-	-
	Issued	1,410	1,613	39	41	309	384
QLD CCC	Made	50	28	-	-	8	7
	Refused	-	-	-	-	-	-
	Issued	50	28	-	-	8	7
QLD Police	Made	274	297	-	-	43	52
	Refused	-	-	-	-	-	-
	Issued	274	297	-	-	43	52
SA Police	Made	58	62	-	-	3	3
	Refused	-	-	-	-	-	-
	Issued	58	62	-	-	3	3
TAS Police	Made	20	22	-	-	1	-
	Refused	-	-	-	-	-	-
	Issued	20	22	-	-	1	-
VIC Police	Made	196	170	11	5	20	10
	Refused	-	-	-	-	-	-
	Issued	196	170	11	5	20	10
WA Police	Made	320	364	-	-	22	33
	Refused	-	7	-	-	-	-
	Issued	320	357	-	-	22	33
TOTAL	**Made**	**3,529**	**3,573**	**52**	**46**	**763**	**747**
	Refused	**5**	**12**	**0**	**0**	**1**	**0**
	Issued	**3,524**	**3,561**	**52**	**46**	**762**	**747**

Warrants that authorise entry on to premises

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 apply for this type of warrant on rare occasions.

Sections 100(1)(d) and 100(2)(d) of the TIA Act provide that this report must set out the relevant statistics about applications for interception warrants made by an agency during the year that included requests that the warrants authorise entry on premises.

Table 5 presents this information. In 2018–19, three interception warrants issued to the AFP authorised entry on to premises to carry out telecommunications interception.

Table 5: Applications for telecommunications interception warrants authorising entry on premises – sections 100(1)(d) and 100(2)(d)

Agency	Relevant statistics	Warrants authorising entry on premises	
		17 / 18	18 / 19
AFP	Made	-	3
	Refused	-	-
	Issued	-	3
TOTAL	**Made**	**-**	**3**
	Refused	**-**	**-**
	Issued	**-**	**3**

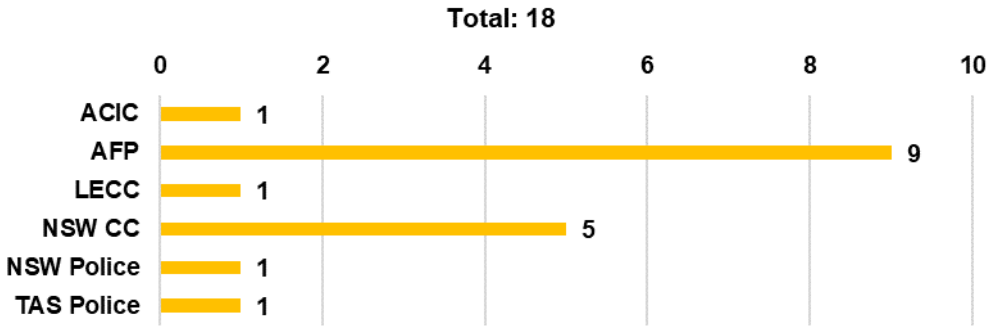
Conditions or restrictions on warrants

Issuing authorities can place conditions or restrictions on an interception warrant. 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.

Sections 100(1)(e) and 100(2)(e) of the TIA Act provide that this report must set out how many interception warrants issued on applications made by an agency during the year specified conditions or restrictions relating to interceptions under the warrants.

Figure 1 presents this information. In 2018–19, 18 interception warrants were issued with a condition or restriction.

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



Effectiveness of telecommunications interception warrants

Sections 102(1)(a) and 102(2)(a) of the TIA Act provide that this report must set out for each agency how many arrests were made during that year in connection with the performance by the agency of its functions and on the basis of information that was or included lawfully intercepted information.

Agencies have also been asked to report on the number of times their lawfully intercepted information culminated in an arrest by another agency, separately from the number of arrests made by the agency that carried out the interception itself. This change removes the risk that arrest numbers will be duplicated due to multiple agencies reporting on the same arrest. This change also shows outcomes from agencies that do not have arrest powers themselves but whose lawfully intercepted information ultimately leads to an arrest by another agency.

Sections 102(1)(b)-(c) and 102(2)(b)-(c) provide that this report must set out the categories of the prescribed offences proceedings by way of prosecutions for which ended during that year, being proceedings in which, according to the records of the agency, lawfully intercepted information was given in evidence; and in relation to each of those categories the number of such offences in that category and the number of such offences in that category in respect of which convictions were recorded.

Tables 6, 7 and 8 provide this information. In 2018–19 there were 2,588 arrests based on lawfully intercepted information. There were also 5,030 prosecutions and 3,400 convictions where lawfully intercepted material was given in evidence.

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 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 full effectiveness of interception in leading to successful prosecutions, 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, eliminating the need for intercepted information to be admitted into evidence.

Table 6: Arrests on the basis of lawfully intercepted information – sections 102(1)(a) and 102(2)(a)

Agency	17 / 18		18 / 19	
	Number of arrests by agency	Number of times lawfully intercepted information culminated in arrest by another agency	Number of arrests by agency	Number of times lawfully intercepted information culminated in arrest by another agency
ACIC	-	99	-	30
ACLEI	2	-	-	1
AFP	165	100	169	166
CCC (WA)	-	-	-	-
IBAC	-	2	-	-
ICAC (SA)	-	-	2	-
NT Police	45	-	16	-
NSW CC	-	70	-	69
NSW Police	763	-	1,218	58
QLD CCC	39	10	24	1
QLD Police	606	-	423	-
SA Police	46	5	36	-
TAS Police	15	-	26	-
VIC Police	337	70	280	70
WA Police	411	-	394	-
TOTAL	**2,429**	**356**[8]	**2,588**	**395**

[8] Correction for 2017–18: In 2017–18 some agencies reported the same arrests under both columns of this table. 2017–18 statistics for the number of times lawfully intercepted information culminated in arrest have been amended for the ACLEI, NT Police, TAS Police and WA Police to properly separate out arrests made by the agency, and times lawfully intercepted information from one agency culminated in an arrest by another agency.

Table 7: Prosecutions per offence category in which lawfully intercepted information was given in evidence – sections 102(1)(b)-(c) and 102(2)(b)-(c)

Category	ACIC	ACLEI	AFP	CCC (WA)	IBAC	ICAC (NSW)	ICAC (SA)	LECC	NT Police	NSW CC	NSW Police	QLD CCC	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
ACIC special investigations	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**0**
Administration of justice / government offences	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**1**
Assisting person to escape or dispose of proceeds	-	-	-	-	-	-	-	-	-	4	3	-	-	-	-	-	-	**7**
Bribery or corruption	-	1	3	-	6	-	1	-	-	1	18	3	-	2	-	2	45	**82**
Cartel offences	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**0**
Child pornography offences	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	15	**15**
Conspire/aid/abet serious offence	-	-	-	-	-	-	1	-	-	-	15	-	-	1	-	1	14	**32**
Cybercrime offences	-	-	6	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**6**
Espionage and foreign interference	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**0**
Kidnapping	-	-	-	-	-	-	-	-	-	-	39	-	-	-	-	3	-	**42**
Loss of life	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	3	-	**3**
Money laundering	1	-	20	-	-	-	-	-	-	124	2	-	-	1	-	-	16	**164**
Murder	-	-	-	-	-	-	-	-	-	13	25	-	-	-	-	9	12	**59**
Offences against the TIA Act	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**0**
Offences involving planning and organisation	-	-	-	-	-	-	-	-	-	-	73	-	-	-	-	20	534	**627**
Organised crime	-	-	-	-	-	-	-	-	-	-	11	-	-	4	-	-	-	**15**
Other offence punishable by 3 years to life	-	1	26	-	-	-	-	1	-	-	120	2	82	-	-	44	-	**276**
People smuggling and related	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**0**
Serious arson	-	-	-	-	-	-	-	-	-	-	9	-	-	-	-	3	-	**12**

Serious damage to property	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	-	15	**16**
Serious drug offence and/or trafficking	1	-	218	-	2	-	-	-	15	88	458	-	158	26	1	78	2,231	**3,276**
Serious fraud	-	-	5	-	1	-	-	-	-	5	70	-	18	-	-	5	-	**104**
Serious loss of revenue	-	-	16	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**16**
Serious personal injury	-	-	-	-	-	-	-	-	-	-	171	-	2	-	-	22	10	**205**
Telecommunications offences	-	-	1	-	-	-	-	-	-	-	61	-	-	-	-	-	-	**62**
Terrorism offences	-	-	7	-	-	-	-	-	-	2	1	-	-	-	-	-	-	**10**
Terrorism financing offences	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**0**
Total	**2**	**2**	**303**	**0**	**9**	**0**	**2**	**1**	**15**	**237**	**1,076**	**5**	**260**	**35**	**1**	**190**	**2,892**	**5,030**

Table 8: Convictions per offence category in which lawfully intercepted information was given in evidence – sections 102(1)(b)-(c) and 102(2)(b)-(c)

Category	ACIC	ACLEI	AFP	CCC (WA)	IBAC	ICAC (NSW)	ICAC (SA)	LECC	NT Police	NSW CC	NSW Police	QLD CCC	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
ACIC special investigations	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**0**
Administration of justice / government offences	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**1**
Assisting person to escape or dispose of proceeds	-	-	-	-	-	-	-	-	-	2	3	-	-	-	-	-	-	**5**
Bribery or corruption	-	1	8	-	4	-	-	-	-	1	3	3	-	4	-	-	22	**46**
Cartel offences	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**0**
Child pornography offences	-	-	-	-	-	-	-	-	-	-	14	-	-	-	-	-	9	**23**
Conspire/aid/abet serious offence	-	-	-	-	-	-	-	-	-	-	8	-	-	-	-	1	9	**18**
Cybercrime offences	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**0**
Espionage and foreign interference	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**0**
Kidnapping	-	-	-	-	-	-	-	-	-	-	2	-	-	-	-	3	-	**5**

Loss of life	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	3	-	**3**
Money laundering	1	-	13	-	-	-	-	-	-	45	2	-	-	1	-	-	7	**69**
Murder	-	-	1	-	-	-	-	-	-	8	14	-	-	-	-	2	4	**29**
Offences against the TIA Act	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**0**
Offences involving planning and organisation	-	-	-	-	-	-	-	-	-	-	55	-	-	-	-	20	372	**447**
Organised crime	-	-	-	-	-	-	-	-	-	-	10	-	-	3	-	-	-	**13**
Other offence punishable by three years to life	-	1	47	-	-	1	2	-	-	-	99	1	79	-	-	44	-	**274**
People smuggling and related	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**0**
Serious arson	-	-	-	-	-	-	-	-	-	-	4	-	-	-	-	2	-	**6**
Serious damage to property	-	-	-	-	-	-	-	-	-	-	5	-	-	-	-	-	5	**10**
Serious drug offence and/or trafficking	1	-	74	-	2	-	-	-	6	42	189	-	154	23	1	53	1,675	**2,220**
Serious fraud	-	-	9	-	1	-	-	-	-	2	10	-	18	-	-	2	-	**42**
Serious loss of revenue	-	-	3	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**3**
Serious personal injury	-	-	-	-	-	-	-	-	-	-	128	-	-	-	-	22	3	**153**
Telecommunications offences	-	-	-	-	-	-	-	-	-	-	22	-	-	-	-	-	-	**22**
Terrorism offences	-	-	8	-	-	-	-	-	-	2	1	-	-	-	-	-	-	**11**
Trafficking in prescribed substances	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**0**
Total	**2**	**2**	**164**	**0**	**7**	**1**	**2**	**0**	**6**	**102**	**569**	**4**	**251**	**31**	**1**	**152**	**2,106**	**3,400**

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 conduct constituting 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.

Sections 100(1)(ea) and 100(2)(ea) provide that this report must set out the relevant statistics about applications, telephone applications and renewal applications for named person warrants, and how many named person warrants issued on applications made by an agency during the year specified conditions or restrictions relating to interceptions under the warrants.

Table 9 and Figure 2 present this information. In 2018–19, 636 named person warrants were issued, a decrease from the 2017–18 reporting period in which 691 named person warrants were issued.

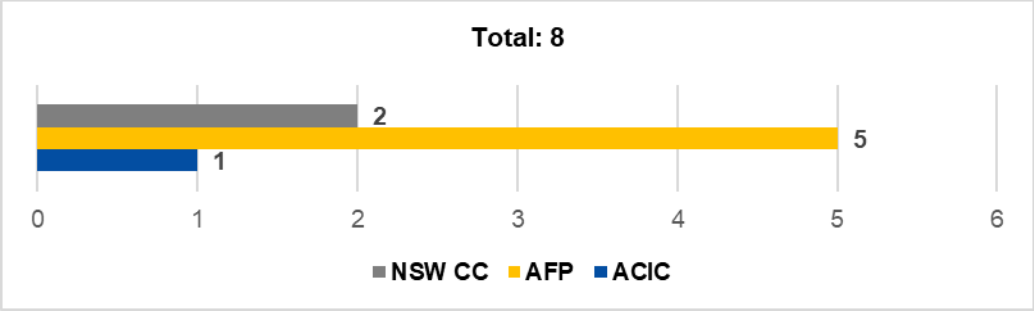
Table 9: Original applications for named person warrants, telephone applications for named person warrants, and renewal applications – sections 100(1)(ea) and 100(2)(ea)

Agency	Relevant Statistics	Applications for named person warrants		Telephone applications for named person warrants		Renewal applications for named person warrants	
		17 / 18	18 / 19	17 / 18	18 / 19	17 / 18	18 / 19
ACIC	Made	88	55	-	-	12	10
	Refused	-	-	-	-	-	-
	Issued	88	55	-	-	12	10
AFP	Made	245	186	-	-	79	53
	Refused	-	-	-	-	-	-
	Issued	245	186	-	-	79	53
CCC (WA)	Made	14	1	-	-	7	-
	Refused	-	-	-	-	-	-
	Issued	14	1	-	-	7	-
IBAC	Made	2	2	-	-	1	-
	Refused	-	-	-	-	-	-
	Issued	2	2	-	-	1	-
NT Police	Made	3	1	-	-	-	-

Agency	Relevant Statistics	Applications for named person warrants		Telephone applications for named person warrants		Renewal applications for named person warrants	
		17 / 18	18 / 19	17 / 18	18 / 19	17 / 18	18 / 19
	Refused	-	-	-	-	-	-
	Issued	3	1	-	-	-	-
NSW CC	Made	67	66	-	-	33	19
	Refused	-	-	-	-	-	-
	Issued	67	66	-	-	33	19
NSW Police	Made	87	83	-	-	31	26
	Refused	-	-	-	-	-	-
	Issued	87	83	-	-	31	26
QLD CCC	Made	7	3	-	-	1	1
	Refused	-	-	-	-	-	-
	Issued	7	3	-	-	1	1
QLD Police	Made	56	55	-	-	5	11
	Refused	-	-	-	-	-	-
	Issued	56	55	-	-	5	11
SA Police	Made	4	4	-	-	-	1
	Refused	-	-	-	-	-	-
	Issued	4	4	-	-	-	1
TAS Police	Made	3	5	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	3	5	-	-	-	-
VIC Police	Made	52	53	1	1	8	4
	Refused	-	-	-	-	-	-
	Issued	52	53	1	1	8	4
WA Police	Made	63	122	-	-	4	13
	Refused	-	-	-	-	-	-
	Issued	63	122	-	-	4	13
Total	**Made**	**691**	**636**	**1**	**1**	**181**	**138**
	Refused / Withdrawn	**-**	**-**	**-**	**-**	**-**	**-**
	Issued	**691**	**636**	**1**	**1**	**181**	**138**

In 2018–19, eight named person warrants were issued with a condition or restriction.

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



Sections 100(1)(eb) and 100(2)(eb) of the TIA Act provide that this report must set out in relation to all named person warrants issued during the year on applications made by each agency, the number of services intercepted in the categories outlined in Table 10. Consistent with previous reporting periods, in 2018–19 the majority of named person warrants were for the interception of between two to five telecommunications services.

Table 10: Number of telecommunications services intercepted under named person warrants – sections 100(1)(eb) and 100(2)(eb)

Agency	Number of services							
	1 service Only		2 – 5 services		6 – 10 services		10+ services	
	17 / 18	18 / 19	17 / 18	18 / 19	17 / 18	18 / 19	17 / 18	18 / 19
ACIC	27	20	53	28	3	7	1	1
AFP	68	55	158	113	13	13	-	1
CCC (WA)	4	-	9	-	1	-	-	1
IBAC	-	-	2	2	-	-	-	-
NT Police	-	-	2	1	1	-	-	-
NSW CC	25	37	34	29	8	-	-	-
NSW Police	16	14	35	43	6	-	-	2
QLD CCC	2	1	5	2	-	-	-	-
QLD Police	17	14	38	37	1	4	-	-
SA Police	-	3	4	1	-	-	-	-
TAS Police	1	2	2	2	-	1	-	-
VIC Police	5	9	45	35	2	3	-	-
WA Police	18	39	42	81	3	2	-	-
TOTAL	**183**	**194**	**429**	**374**	**38**	**30**	**1**	**5**

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.

Section 100(1)(ec)(i)-(iii) requires 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 3 and Table 11 outline the number of services intercepted under the different types of named person warrants and should be read in conjunction with Table 9, which provides the total number of named person warrants issued.

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

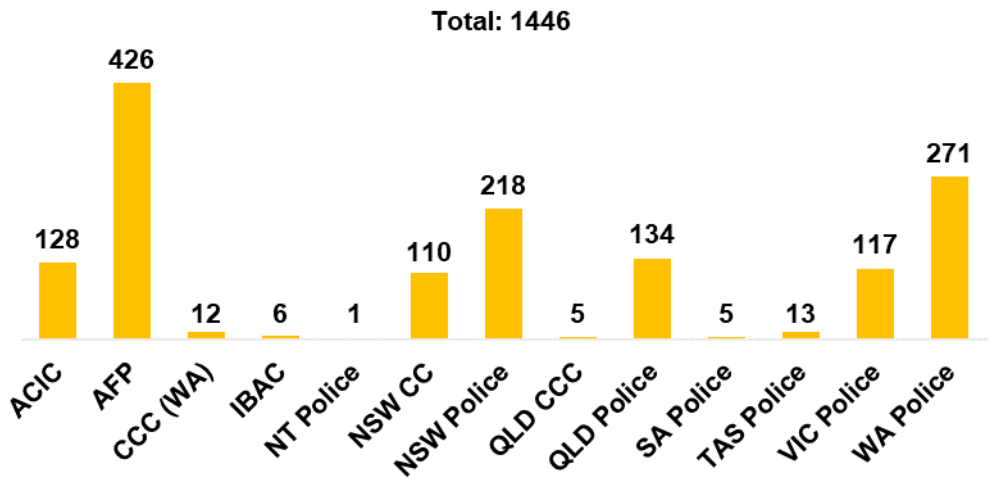


Table 11 shows that in 2018–19, device based named person warrants were used by only a small number of agencies. This is consistent with the 2017–18 reporting period.

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

Agency	Devices		Services	
	17 / 18	18 / 19	17 / 18	18 / 19
ACIC	5	4	16	4
AFP	66	48	-	291
NSW CC	-	7	-	-
NSW Police	23	15	87	18
VIC Police	2	6	6	-
TOTAL	**96**	**80**	**109**	**313**

B-Party warrants

Definition

A **'B-Party warrant'** is a telecommunications service 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 the interception of communications from that person's telecommunications services would not otherwise be possible.

Sections 100(1)(ed) and 100(2)(ed) provide that this report must set out the relevant statistics about applications, telephone applications and renewal applications for B-party warrants, and how many B-Party warrants issued on applications made by an agency during the year included requests to authorise entry on premises, or specified conditions or restrictions relating to interceptions under the warrants.

This information is presented in Tables 12 and 13. In 2018–19, 118 B-Party warrants were issued to interception agencies. This represents a decrease from the 152 B-Party warrants issued in 2017–18.

Table 12: Applications for B-Party warrants, telephone applications for B-Party warrants, and renewal applications – sections 100(1)(ed) and 100(2)(ed)

Agency	Relevant Statistics	Applications for B-Party Warrants		Telephone applications for B-Party warrants		Renewal applications for B-Party warrants	
		17 / 18	18 / 19	17 / 18	18 / 19	17 / 18	18 / 19
AFP	Made	113	66	-	-	76	50
	Refused	-	-	-	-	-	-
	Issued	113	66	-	-	76	50
NSW CC	Made	4	3	-	-	2	-
	Refused	-	-	-	-	-	-
	Issued	4	3	-	-	2	-
NSW Police	Made	30	46	10	5	2	2
	Refused	-	-	-	-	-	-
	Issued	30	46	10	5	2	2
QLD Police	Made	5	-	-	-	2	-
	Refused	-	-	-	-	-	-
	Issued	5	-	-	-	2	-
SA Police	Made	-	1	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	-	1	-	-	-	-
VIC Police	Made	-	2	-	-	-	-

Agency	Relevant Statistics	Applications for B-Party Warrants		Telephone applications for B-Party warrants		Renewal applications for B-Party warrants	
		17 / 18	18 / 19	17 / 18	18 / 19	17 / 18	18 / 19
	Refused	-	-	-	-	-	-
	Issued	-	2	-	-	-	-
	Made	**152**	**118**	**10**	**5**	**82**	**52**
TOTAL	**Refused**	**-**	**-**	**-**	**-**	**-**	**-**
	Issued	**152**	**118**	**10**	**5**	**82**	**52**

In 2018–19, no B-Party warrants were issued with conditions or restrictions or authorised entry on premises.

Table 13: B-Party warrants issued with conditions or restrictions – sections 100(1)(ed) and 100(2)(ed)

Agency	B-party warrants specifying conditions or restrictions	
	17 / 18	18 / 19
NSW Police	1	-
TOTAL	**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.

Sections 101(1)(a)-(d) and 101(2)(a)-(d) of the TIA Act provide that this report must set out for each agency 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 – sections 101(1)(a)-(d) and 101(2)(a)-(d)

Agency	Duration of original telecommunications warrants		Duration of renewal 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)
ACIC	89	55	90	82
ACLEI	78	49	90	69
AFP	83	68	78	66
CCC (WA)	86	28	-	-
IBAC	86	82	90	90
ICAC (NSW)	90	88	78	62
ICAC (SA)[9]	70	50	75	-
LECC	90	90	90	55
NT Police	88	55	-	-
NSW CC	77	58	83	73
NSW Police	42	34	51	44
QLD CCC	80	74	74	73
QLD Police	78	59	80	68
SA Police	78	57	90	67
TAS Police	81	60	90	66
VIC Police	73	53	77	46
WA Police	80	46	90	69
AVERAGE	**78**	**59**	**82**	**66**

[9] As all of ICAC SA's renewals of telecommunications interception warrants were still in force at the end of the reporting period, an average period the warrants were in force during 2018–19 is unable to be calculated.

A single B-Party warrant can be in force for up to 45 days. Sections 101(1)(da) and 102(2)(da) of the TIA Act provide that this report must set out for each agency the average length of time for which B-Party warrants – including renewals – were specified to be in force when issued and the average length of time they were actually in force during the reporting period.

Table 15: Duration of original and renewal B-Party warrants – sections 101(1)(da) and 102(2)(da)

Agency	Duration of original telecommunications B-party warrants		Duration of renewal 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	45	42	45	44
NSW CC	45	45	-	-
NSW Police	32	22	39	28
SA Police	3	3	-	-
VIC Police	45	45	-	-
AVERAGE	**34**	**31**	**42**	**36**

Final renewals

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. Sections 101(1)(e) and 101(2)(e) of the TIA Act provide that this report must set out how many final renewals ceased during that year 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 presents information on the number of final renewals of warrants by agencies.

Table 16: Number of final renewals – sections 101(1)(e) and 101(2)(e)

Agency	90 days		150 days		180 days	
	17 / 18	18 / 19	17 / 18	18 / 19	17 / 18	18 / 19
ACIC	6	3	2	4	7	2
ACLEI	-	1	1	1	2	2
AFP	32	5	17	29	73	41
CCC (WA)	1	-	7	-	4	-
IBAC	3	-	2	6	-	-
ICAC (NSW)	-	-	4	-	-	3
LECC	1	4	-	1	2	-
NSW CC	2	2	4	9	4	8
NSW Police	116	129	12	20	25	43
QLD CCC	6	2	1	5	1	-
QLD Police	14	19	7	17	7	6
SA Police	3	-	-	3	-	-
VIC Police	11	5	-	-	3	-
WA Police	8	12	-	27	1	3
TOTAL	**203**	**182**	**57**	**122**	**129**	**108**

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.

'**Total warrants**' means the number of warrants that were issued to an agency and in force during the year to which the report relates.

Sections 102(3) and 102(4) of the TIA Act provide that this report must set out for each agency, the percentage of eligible warrants against the number of total warrants during the year.

Table 17 presents this information. In 2018–19, 69 per cent of total warrants were eligible warrants.

Table 17: Percentage of eligible warrants – sections 102(3) and 102(4)

Agency	Total number of warrants	Number of eligible warrants	%
ACIC	152	75	49
ACLEI	14	5	36
AFP	775	461	59
CCC (WA)	15	-	0
IBAC	20	13	65
ICAC (NSW)	19	12	63
ICAC (SA)	23	8	35
LECC	21	3	14
NT Police	22	10	45
NSW CC	154	83	54
NSW Police	1,804	1,440	80
QLD CCC	37	28	76
QLD Police	334	319	96
SA Police	69	45	65
TAS Police	22	13	59
VIC Police	203	112	55
WA Police	406	204	50
TOTAL / AVERAGE	**4,090**	**2,831**	**69**

Interception without a warrant

Under sections 7(4) and (5) of the TIA Act, the Australian Federal Police and the police forces of States and the Northern Territory can undertake interception without a warrant in limited circumstances. Section 102A of the TIA Act provides that this report must set out, for each of those agencies, the number of occasions on which an officer or staff member of the agency intercepted a communication in reliance on sections 7(4) or (5).

Table 18 presents this information on interceptions under section 7(5) of the TIA Act. In 2018–19, there were no instances where agencies intercepted communications under sections 7(4) or (5) of the TIA Act without a warrant.

Table 18: Interception without a warrant where a person consents – section 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	
	17 / 18	18 / 19	17 / 18	18 / 19	17 / 18	18 / 19	17 / 18	18 / 19
NSW Police	-	-	1	-	-	-	-	-
TOTAL	-	-	1	-	-	-	-	-

International assistance

Section 102B of the TIA Act provides that this report must set out the number of occasions on which lawfully intercepted information or interception warrant information was provided to:

- a foreign country under sections 68(l) or 68A of the TIA Act in connection with an authorisation under section 13A(1) of the *Mutual Assistance in Criminal Matters Act 1987*;
- the International Criminal Court under sections 68(la) or 68A of the TIA Act in connection with an authorisation under section 69A of the *International Criminal Court Act 2002*;
- a War Crimes Tribunal under sections 68(lb) or 68A of the TIA Act in connection with an authorisation under section 25A of the *International War Crimes Tribunals Act 1995.*

In 2018–19, there were two occasions in which lawfully intercepted information was provided to a foreign country under section 13A(1) of the *Mutual Assistance in Criminal Matters Act 1987*.

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. Section 103(ac) of the TIA Act provides that this report must set out for each agency the number (if any) of interceptions carried out on behalf of other agencies.

Table 19: Number of interceptions carried out on behalf of other agencies – section 103 (ac)

Interception carried out by:	Interception carried out on behalf of:	Number of interceptions
ACIC	QLD CCC	29
AFP	ACLEI	8
CCC WA	ICAC (SA)	12
IBAC	NSW CC	6
	LECC	3
	SA ICAC	5
	CCC (WA)	1
LECC	ACLEI	3
VIC Police	TAS Police	22
TOTAL		**89**

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 – sections 103(a) and 103(aa).

Agency	Total expenditure	Average expenditure
ACIC	$7,566,514	$57,322
ACLEI	$701,935	$63,812
AFP	$14,765,668	$23,290
CCC (WA)	$1,093,807	$42,070
IBAC	$882,457	$51,909
ICAC (NSW)	$502,749	$26,460
ICAC (SA)	$218,248	$11,487
LECC	$892,055	$49,559
NT Police	$812,652	$47,803
NSW CC	$2,146,551	$16,386
NSW Police	$9,014,556	$5,589
QLD CCC	$1,589,339	$56,762
QLD Police	$6,711,862	$22,599
SA Police	$3,534,555	$57,009
TAS Police	$275,227	$12,510
VIC Police	$1,068,690	$6,286
WA Police	$3,999,043	$11,202
TOTAL / AVERAGE	**$55,775,908**	**$33,062**

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 ($)
ACIC	$5,717,989	$61,048	$349,491	$1,437,986	**$7,566,514**
ACLEI	$598,860	$54,246	-	48,829	**$701,935**
AFP	$9,744,255	$76,701	-	$4,944,711	**$14,765,667**
CCC (WA)	$871,610	$1,579	$91,916	$128,702	**$1,093,807**
IBAC	$675,149	$22,302	$80,079	$104,927	**$882,457**
ICAC (NSW)	$234,523	-	-	$268,226	**$502,749**
ICAC (SA)	$122,256	-	$21,000	$74,992	**$218,248**
LECC	$649,218	$86,033	$74,873	$81,931	**$892,055**
NT Police	$388,109	$190,020	$155,771	$78,752	**$812,652**
NSW CC	$1,418,158	-	-	$728,393	**$2,146,551**
NSW Police	$5,917,882	$145,405	$47,235	$2,904,044	**$9,014,566**
QLD CCC	$1,037,472	$168,550	$46,270	$337,046	**$1,589,338**
QLD Police	$4,657,639	$991,058	-	$1,063,164	**$6,711,861**
SA Police	$2,301,048	$117,742	$164,237	$951,528	**$3,534,555**
TAS Police	$691,137	$14,072	$1203	$275,228	**$981,640**
VIC Police	$828,945	$16,740	$95,000	$97,005	**$1,037,690**
WA Police	$3,238,543	$557,831	-	$202,669	**$3,999,043**
TOTAL	**$39,092,793**	**$2,503,327**	**$1,127,075**	**$13,728,133**	**$56,451,328**

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 the recording of the call.

Table 22: Emergency service facility declarations – section 103(ad)

Agency	Police	Fire brigade	Ambulance	Emergency services authority	Despatching
Australian Capital Territory	5	-	-	-	3
New South Wales	8	94	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**	**113**	**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 Department of Home Affairs (Home Affairs) with a copy of each telecommunications interception warrant;
- interception agencies to report to the Minister, within three months of a warrant ceasing to be in force, detailing the use made of information obtained by the interception;
- the Secretary of Home Affairs to maintain a General Register detailing the particulars of all telecommunications interception warrants. The Secretary of Home Affairs must provide the General Register to the Minister for inspection every three months; and
- the Secretary of Home Affairs 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 Minister 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 ACIC, the ACLEI, and the AFP relating to interceptions, and the use, dissemination and destruction of intercepted information. The inspections are retrospective, 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 2018.

The Commonwealth Ombudsman is required under the TIA Act to report to the Minister 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 ACIC, the 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 Minister. 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 *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Data Retention Act) introduced additional obligations for these reports to be provided to the Minister 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 ACIC, the ACLEI, and the AFP (two inspections for each agency) – refer to Table 23.

During its review of warrants that expired or were revoked in the period between 1 January and 31 December 2018 the Ombudsman noted there continues to be a satisfactory level of compliance, where agencies demonstrated a good understanding of the requirements of the TIA Act and, with one exception, maintained appropriate disclosure of compliance issues.

The Ombudsman's inspection criteria (see Figures 4 and 5) are:

- Were restricted records properly destroyed in accordance with section 79 of the TIA Act?
- Were the requisite documents kept in connection with the issue of warrants in accordance with section 80 of the TIA Act?
- Were warrant applications properly made and warrants in the correct form in accordance with sections 39(1) and 49 of the TIA Act?
- Were the requisite records kept in connection with interceptions in accordance with section 81 of the TIA Act?
- Were interceptions conducted in accordance with the warrants (section 7) and was any unlawfully intercepted information properly dealt with in accordance with section 63 of the TIA Act?

The Ombudsman may also inspect the records of technical assistance requests, technical assistance notices and technical capability notices given under Part 15 of the Telecommunications Act when the measures have been used in connection with an interception warrant. As the industry assistance measures compliment TIA Act powers, this ensures the Commonwealth Ombudsman can oversight their joint use.

Commonwealth Ombudsman's summary of findings

Table 23: Summary of findings from the two inspections conducted at each Commonwealth agency in 2018–19 – section 103(ae)

Criteria	ACIC	ACLEI	AFP
Were restricted records properly destroyed (s 79)?	Not assessed. The ACIC advised it did not conduct any destruction of restricted records during the inspection.	Not assessed. The ACLEI advised it did not conduct any destruction of restricted records during the inspection.	Four instances of non-compliance.
Were the requisite documents kept in connection with the issue of warrants (s 80)?	Compliant.	Compliant.	Compliant.
Were warrant applications properly made and warrants in the correct form (ss 39(1) and 49)?	Compliant with minor exceptions.	Compliant with minor exceptions.	Compliant with minor exceptions.
Were the 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)?	Two instances of non-compliance.	Compliant.	Two instances of non-compliance.

Commonwealth Ombudsman's findings per Commonwealth agency for warrants expiring between 1 January to 31 December 2018

ACIC

Section 58 of the TIA Act states that the chief officer of an agency must, on the revocation of a warrant, immediately take steps necessary to ensure that interceptions of communications under the warrant are discontinued. Section 59 states that a warrant will not cease to be in force until the instrument of revocation is received by or on behalf of the Secretary of the Department of Home Affairs or when the warrant expires, whichever happens sooner.

At the Ombudsman's first inspection of the ACIC, there were two instances where intercepted information was received by the ACIC after the instrument of revocation

was received on behalf of the Secretary of the Department of Home Affairs, contrary to section 58.

The Ombudsman noted in both instances the interceptions had commenced prior to revocation, when the warrant remained in force. When the Ombudsman raised the issue at the inspection, the ACIC immediately quarantined the affected data. Following the inspection, the ACIC advised they had commenced actions to amend the wording in their Compliance Management System Checklist to reflect the notification requirement under section 59 of the TIA Act.

The Ombudsman also identified one instance where intercepted information was received by the ACIC after the warrant had expired. In this instance, the interception had commenced prior to expiry when the warrant remained in force. When the Ombudsman raised the issue at the inspection, the ACIC immediately quarantined the affected data.

ACLEI

At the Ombudsman's second inspection of ACLEI, it was identified that an authorisation instrument ACLEI relied on to exercise the authority of warrants contained wording that appeared to revoke all previous authorisations under section 55(3) of the TIA Act, rather than only the smaller group of authorisations relevant to ACLEI staff, as it had intended. Following the Ombudsman's inspection, ACLEI advised it did not consider the wording of the authorisation instrument had this effect.

To avoid any future ambiguity, ACLEI has since updated the wording of its authorisations. ACLEI consulted the Ombudsman's Office on these changes and the Ombudsman's Office have made suggestions to ACLEI in response. While noting ACLEI's position and its action to update the authorisation template, the Ombudsman thought it appropriate that ACLEI inform its partner agencies about this matter and advise those agencies of the remedial action it has taken to remove any future ambiguity.

AFP

At the Ombudsman's first inspection of the AFP, there were two instances where original copies of lawfully intercepted information were not destroyed at the time of the inspection, despite being certified for destruction more than two months prior to the inspection. At the inspection the Ombudsman identified two data storage discs in the storage area for warrants, however the discs were located with the records for another warrant. The Ombudsman states this may explain why the discs were not destroyed during the relevant destruction round. Following the inspection, the AFP advised the original copies had been destroyed.

At the second inspection of the AFP, the Ombudsman identified two instances where restricted records did not appear to have been destroyed in accordance with the TIA Act. The Ombudsman also identified an inconsistency with the AFP's destruction processes and its written destruction procedures. The Ombudsman suggested the AFP update its procedures for destruction of records, specifically 'digital' restricted records, to achieve compliance with section 79 of the TIA Act. Following the inspection, the AFP acknowledged the findings and advised that it will update its written procedures

regarding destructions. The Ombudsman will continue to monitor this issue at future inspections and assess the updated procedures at their next inspection in January 2020.

At the second inspection of the AFP, there was an issue included in the disclosure log of an instance where the AFP communicated lawfully intercepted information to partner agencies. Section 63(1) of the TIA Act restricts the communication of lawfully intercepted information to specific purposes. In this instance, the AFP's communication of the lawfully intercepted information to its partner agencies did not constitute a 'permitted purpose' under the TIA Act and was therefore was done contrary to section 63 of the TIA Act. Despite the AFP being aware of this issue prior to the Ombudsman's inspection, the AFP had not taken any remedial action at the time of the inspection. As a result of the Ombudsman's Office discussing this matter with the AFP during the inspection, the AFP subsequently contacted all partner agency recipients of the communication to request they destroy the information, and provide confirmation once destroyed.

The Ombudsman suggested that AFP amend its policies, procedures and training in relation to the communication of lawfully intercepted information under the Act, to ensure its officers are aware of the circumstances under which such communication can occur and mitigate against future non-compliance. Following the inspection the AFP advised it had received confirmation that the partner agencies had destroyed all product at the time of their initial request. The AFP also disseminated information to its investigators to advise them of the Ombudsman's finding and to remind them of their obligations under the Act.

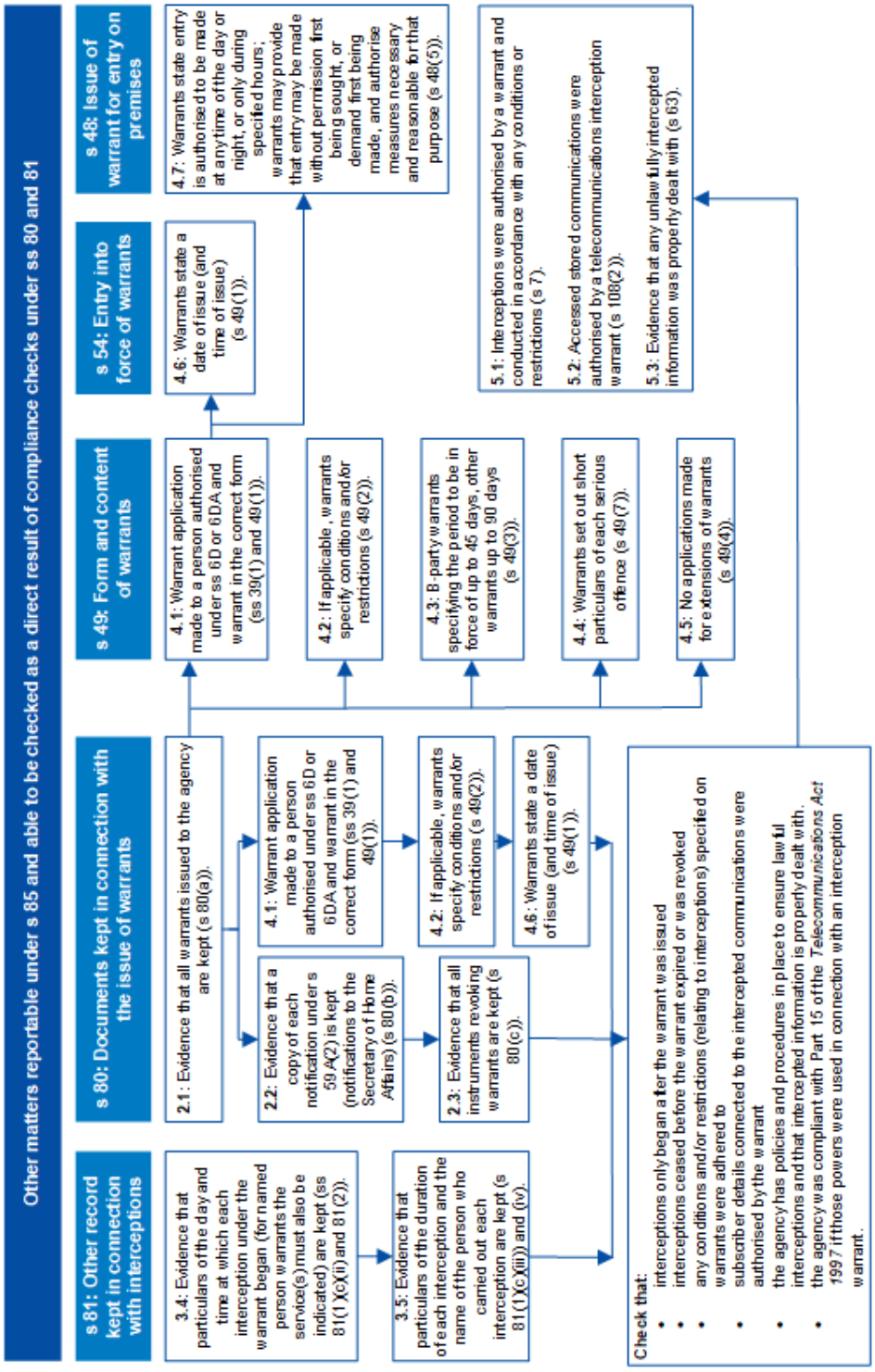
As part of the inspection methodology, the Ombudsman also reports on administrative errors which have resulted in non-compliance, including instances where the consequences may be negligible. The Ombudsman identified, and all agencies disclosed, a number of non-compliances of this nature. The Ombudsman was satisfied that the issues owing to administrative errors were not systemic in nature and those that related to template or form errors have been rectified to achieve future compliance.

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)).	**2.1:** Evidence that all warrants issued to the agency are kept (s 80(a)).	**3.1:** Evidence that each telephone application for a part 2-5 warrant is kept (s 81(1)(a)).
1.2: *Evidence that the restricted records were not destroyed before the agency has received written notice from the Secretary for Home Affairs that the entry in the General Register relating to the warrant has been inspected by the Minister* (s 79(2)).	**2.2:** Evidence that a copy of each notification under s 59A(2) is kept (notifications to the Secretary of Home Affairs) (s 80(b)).	**3.2:** Evidence that statements as to whether applications were withdrawn, refused, or issued on the application are kept. (s 81(1)(b)).
	2.3: Evidence that all instruments revoking warrants are kept (s 80(c)).	**3.3:** Evidence that the particulars of all warrants whose authority is exercised by the agency are kept (s 81)(1)(c)(i).
	2.4: Evidence that a copy of each certificate issued under s 61(4) is kept (*evidentiary certificates*) (s 80(d)).	**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)).
	2.5: Evidence that each authorisation by the chief officer under s 66(2) is kept (*authorisation to receive information under warrants*) (s 80(e)).	**3.5:** Evidence that particulars of the duration of each interception and the name of the person who carried out each interception are kept (ss 81(1)(c)(iii) and (iv).
		3.6: Evidence that particulars of each named person warrant including each service to or from which communications have been intercepted under the warrants are kept (s 81(1)(c)(v)).
		3.7: Evidence that each warrant issued to the agency is kept that relates to restricted records that have at any time been in the agency's possession (s 81(1)(d)(i)).
		3.8: Evidence that particulars of each occasion when the restricted record came to be in the agency's possession are kept (s 81(1)(d)(ii).
		3.9: Evidence that particulars of each occasion when the restricted record ceased to be in the agency's possession are kept (s 81(1)(d)(iii).
		3.10: Evidence that particulars of each other agency from or to which or other person from or to whom the agency received or supplied the restricted record are kept (s 81(1)(d)(iv).
		3.11: Evidence that particulars of each use made by the agency of LII are kept (s 81(1)(e)).
		3.12: Evidence that particulars of each communication of LII by an officer of the agency to a person or body other than such an officer are kept (s 81(1)(f)).
		3.13: Evidence that particulars of when LII was given in evidence in a relevant proceeding in relation to the agency are kept (s 81(1)(g)).

Figure 4: Other Matters reportable under section 85



CHAPTER 2 – STORED COMMUNICATIONS

Applications for stored communications warrants

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 Home Affairs, the Australian Securities and Investments Commission and the Australia Competition and Consumer Commission.

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

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 at least 180 penalty units (currently $37,800) for individuals or 900 penalty units (currently $189,000) for non-individuals such as corporations.

Sections 162(1)(a)-(b) and 162(2)(a)-(b) and (c) of the TIA Act provide that this report must set out the relevant statistics about applications, telephone applications and renewal applications for stored communications warrants that criminal law-enforcement agencies made during the year.

In 2018–19, 1,252 stored communications warrants were issued, representing an increase of 424 on the 828 warrants issued in the 2017–18 period.

Table 24: Applications, telephone applications and renewal applications for stored communications warrants – subsections 162(1)(a)-(b) and 162(2)(a)-(c)

Agency	Relevant statistics	Applications for stored communications warrants		Telephone applications for stored communications warrants		Renewal applications for stored communications warrants	
		17 / 18	18 / 19	17 / 18	18 / 19	17 / 18	18 / 19
ACCC	Made	-	9	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	-	9	-	-	-	-
ACIC	Made	5	2	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	5	2	-	-	-	-
ACLEI	Made	4	-	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	4	-	-	-	-	-
AFP	Made	61	100	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	61	100	-	-	-	-
ASIC	Made	2	-	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	2	-	-	-	-	-
CCC (WA)	Made	-	1	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	-	1	-	-	-	-
Home Affairs	Made	15	9	-	-	-	-
	Withdrawn	-	2	-	-	-	-
	Issued	15	7	-	-	-	-
IBAC	Made	1	3	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	1	3	-	-	-	-
ICAC (NSW)	Made	-	6	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	-	6	-	-	-	-
ICAC (SA)	Made	2	-	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	2	-	-	-	-	-
LECC	Made	1	5	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	1	5	-	-	-	-
NT Police	Made	2	4	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	2	4	-	-	-	-
NSW CC	Made	4	1	-	-	-	-

Agency	Relevant statistics	Applications for stored communications warrants		Telephone applications for stored communications warrants		Renewal applications for stored communications warrants	
		17 / 18	18 / 19	17 / 18	18 / 19	17 / 18	18 / 19
	Refused	-	-	-	-	-	-
	Issued	4	1	-	-	-	-
NSW Police	Made	405	707	4	1	-	-
	Refused	-	-	-	-	-	-
	Issued	405	707	4	1	-	-
QLD CCC	Made	6	3	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	6	3	-	-	-	-
QLD Police	Made	147	165	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	147	165	-	-	-	-
SA Police	Made	14	26	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	14	26	-	-	-	-
TAS Police	Made	43	50	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	43	50	-	-	-	-
VIC Police	Made	90	115	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	90	115	-	-	-	-
WA Police	Made	26	48	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	26	48	-	-	-	-
TOTAL	**Made**	**828**	**1,254**	**4**	**1**	**-**	**-**
	Refused / Withdrawn	**-**	**2**	**-**	**-**	**-**	**-**
	Issued	**828**	**1,252**	**4**	**1**	**-**	**-**

Conditions or restrictions on stored communications warrants

Section 162(2)(d) of the TIA Act provides that this report must set out how many stored communications warrants issued on applications made during the year specified conditions or restrictions relating to access to stored communications under warrants.

Table 25 presents this information. In 2018–19, 732 stored communications warrants were subject to conditions or restrictions.

Table 25: Stored Communications warrants subject to conditions or restrictions – section 162(2)(d)

Agency	17 / 18	18 / 19
NSW CC	**-**	1
NSW Police	405	707
QLD CCC	3	-
SA Police	14	24
TOTAL	**422**	**732**

Effectiveness of stored communications warrants

Section 163(a)-(b) of the TIA Act provide that this report must set out how many arrests were made during the year on the basis of information that was, or included, lawfully accessed information and how many proceedings ended during that year that were proceedings in which lawfully accessed information was given in evidence.

Table 26 presents this information. In 2018–19, criminal law-enforcement agencies made 565 arrests, conducted 884 proceedings and obtained 280 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 – section 163(a)-(b)

Agency	Arrests		Proceedings		Convictions	
	17 / 18	18 / 19	17 / 18	18 / 19	17 / 18	18 / 19
ACIC	1	2	-	-	-	-
ACLEI	1	-	1	-	2	-
AFP[10]	20	2	11	1	5	4
Home Affairs	1	2	1	-	1	-
IBAC	-	-	1	-	1	-
NT Police	-	1	-	-	-	-
NSW CC	4	-	3	-	3	-
NSW Police	215	383	430	843	164	227
QLD CCC	-	7	-	-	-	-
QLD Police	107	108	163	14	160	14
SA Police	11	5	4	3	1	5
TAS Police	3	2	-	2	3	2
VIC Police	49	53	8	21	7	28
TOTAL	**412**	**565**	**622**	**884**	**347**	**280**

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 period, or an even later reporting period.

[10] Correction for 2017-18: AFP figures relating to proceedings and convictions on the basis of lawfully accessed information have been amended from 0 and 14 to 11 and 5 respectively due to a transposition error in the 2017-18 Annual Report. As such, the total figures have also been amended.

Preservation notices

Under Part 3-1A 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 TIA Act provides for three types of preservation notices:

- *Historic domestic preservation notices* – requires the preservation of all communications held by the carrier from the time they receive the notice until the end of that day. The carrier must preserve this data for up to 90 days.
- *Ongoing domestic preservation notices* – requires the preservation of all communications held by the carrier from the time the notice is received until the end of the 29th day after the day the notice is received. The carrier must preserve this data for up to 90 days. Only interception agencies may give ongoing domestic preservation notices.
- *Foreign preservation notices* – requires the preservation of all stored communications that a carrier holds from the time they receive the notice until the end of the day they received the notice, that relate to the specified person and in connection with the contravention of foreign laws. Only the AFP may give foreign preservation notices.

Domestic preservation notices must be revoked if the person specified in the notice is no longer under investigation or the agency decided not to apply for a warrant to access stored communications.

Foreign preservation notices must be revoked if 180 days has elapsed since the carrier was given the notice and either no request to the Attorney-General has been made, or a request made has been refused.

Sections 161A(1) and (2) of the TIA Act provides that this report must set out the relevant statistics about domestic preservation notices and revocation notices that were given by the agency during the year.

Table 27 presents this information. In 2018-19, 2,216 domestic preservation notices were given, an increase of 571 on the 1,645 given in 2017-18.

Table 27: Domestic preservation notices – section 161A(1)

Agency	Domestic preservation notices issued		Domestic preservation revocation notices issued	
	17 / 18	18 / 19	17 / 18	18 / 19
ACCC	-	12	-	3
ACIC	26	8	7	1
ACLEI	3	-	-	-
AFP	149	182	67	66
ASIC	94	-	-	-
CCC (WA)	-	3	-	1
Home Affairs	18	10	2	1
IBAC	1	24	-	6
ICAC (NSW)	2	12	-	2
ICAC (SA)	10	11	2	6
LECC	9	8	7	-
NT Police	36	45	30	21
NSW CC	6	1	1	-
NSW Police	558	909	113	180
QLD CCC	26	25	7	6
QLD Police	306	373	71	136
SA Police	88	127	57	82
TAS Police	93	153	51	82
VIC Police	141	165	31	41
WA Police	79	148	49	89
TOTAL	**1,645**	**2,216**	**495**	**723**

Section 161A(2) of the TIA Act provides that this report must set out the relevant statistics about foreign preservation notices and revocation notices given by the AFP during the year. In 2018–19, the AFP reported that ten foreign preservation notices were given with two revocations.

Table 28: Foreign preservation notices – subsection 161A(2)

Agency	Foreign preservation notices given		Foreign preservation revocation notices given	
	17 / 18	18 / 19	17 / 18	18 / 19
AFP	8	10	5	2

International assistance

Section 162(1)(c) provides that this report must set out the number of stored communications warrants issued as a result of international assistance applications.

Definition

An **'international offence'** is:

- an offence against a law of a foreign country; or
- a crime within the jurisdiction of the International Criminal Court; or
- a War Crimes Tribunal Offence.

Section 162(1)(d) requires the report must list, for each international offence in respect of which a stored communications warrant was issued as a result of an international assistance application made by the agency during the year – the offence under a law of the Commonwealth, or of a State or Territory that is of the same nature as, or substantially similar to, the international offence.

Table 29 presents this information. In 2018–19, no agencies made an application for a stored communications warrant as a result of an international assistance application.

Table 29: Applications for stored communications warrants as a result of international assistance applications – subsection 162(1)(c)

Agency	Relevant statistics	Applications for stored communications warrants	
		17 / 18	18 / 19
AFP	Made	10	-
	Refused	-	-
	Issued	10	-
TOTAL	**Made**	**10**	**-**
	Refused	**-**	**-**
	Issued	**10**	**-**

Section 163A of the TIA Act provides that this 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 in connection with an authorisation under section 13A(1) of the *Mutual Assistance in Criminal Matters Act 1987*;
- the International Criminal Court in connection with an authorisation under section 69A(1) of the *International Criminal Court Act 2002*;
- a War Crimes Tribunal in connection with an authorisation under section 25A(1) of the *International War Crimes Tribunals Act 1995.*

In 2018–19, there were no occasions in which lawfully accessed information or stored communications warrant information was provided to a foreign country, the International Criminal Court or a War Crimes Tribunal.

Ombudsman inspection report

The Commonwealth Ombudsman inspects the preservation notices and stored communications access record of all criminal law-enforcement agencies. Due to changes made through the Data Retention Act, this annual report no longer includes information on inspections concerning stored communications and preservation notices. Under section 186J of the TIA Act, the Commonwealth Ombudsman continues to have a statutory obligation to report on the results of these inspections to the Minister.

The Minister must cause a copy of the Ombudsman's inspection reports to be laid before each House of Parliament within 15 sitting days of that House after the Minister receives the inspection report. This requirement will ensure the Parliament and public have visibility of the inspection results outside of the annual report.

The Ombudsman's inspection reports on agency compliance with chapters three and four of the TIA Act can be found at <www.ombudsman.gov.au>

CHAPTER 3 – TELECOMMUNICATIONS DATA

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.

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 and to locate a missing person.

Definition

The definition of **'enforcement agency'** is 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 Home Affairs, the Australian Securities and Investments Commission, and the Australian Competition and Consumer Commission.

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.

Enforcement agencies can access existing 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 *criminal law-enforcement agencies* 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 one the relevant telecommunications service provider receives the request and is effective for 45 days or less.

Existing data – enforcement of the criminal law

Section 178 of the TIA Act provides that an authorised officer of an enforcement agency can authorise the disclosure of telecommunications data if he or she is satisfied it is reasonably necessary for the enforcement of the criminal law.

Section 186(1)(a) of the TIA Act provides that this report must set out the number of authorisations made under section 178 by agencies during the year.

Table 30 provides this information. In 2018–19, 291,353 authorisations were made by agencies under section 178, a decrease of 4,426 from the 295,779 authorisations made in 2017–18.

Table 30: Number of authorisations made by an enforcement agency for access to existing information or documents in the enforcement of a criminal law – section 186(1)(a)

Agency	Authorisations	
	17 / 18	18 / 19
ACCC	40	100
ACIC	7,498	6,536
ACLEI	413	393
AFP	19,432	16,818
ASIC	1,869	1,800
CCC (WA)	123	122
Home Affairs	3,598	3,283
IBAC	701	539
ICAC (NSW)	291	298
ICAC (SA)	288	220
LECC	376	459
NT Police	2,105	3,543
NSW CC	2,893	3,323
NSW Police	99,222	105,199
QLD CCC	1,271	1,009
QLD Police	25,014	23,693
SA Police	10,641	5,477
TAS Police	8,554	7,759
VIC Police	90,112	87,680
WA Police	21,338	23,102
TOTAL	**295,779**	**291,353**

Existing data – assist in locating a missing person

Section 178A of the TIA Act provides that an authorised officer of the Australian Federal Police or the Police Force of a State or the Northern Territory can authorise the disclosure of telecommunications data if he or she is satisfied it is reasonably necessary for the purposes of finding a person that has been reported missing.

Section 186(1)(aa) of the TIA Act provides that this report must set out the number of authorisations made under section 178A by agencies during the year.

Table 31 presents this information. In 2018–19, 2,589 authorisations were made by agencies under section 178A, a decrease of 632 from the 3,221 authorisations made in 2017–18.

Table 31: Number of authorisations made for access to existing information or documents for the location of missing persons – section 186(1)(aa)

Agency	Authorisations	
	17 / 18	18 / 19
AFP	178	194
NT Police	15	31
NSW Police	1,015	1,228
QLD Police	289	199
SA Police	160	79
TAS Police	114	168
VIC Police	1,345	447
WA Police	105	243
TOTAL	**3,221**	**2,589**

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

Section 179 of the TIA Act provides that an authorised officer of an enforcement agency can authorise the disclosure of telecommunications data if he or she is satisfied it is reasonably necessary for the enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue. Section 186(1)(b) of the TIA Act provides that this report must set out the number of authorisations made under section 179 by agencies during the year.

Table 32 presents this information. In 2018–19, 1,749 authorisations were made by agencies under section 179, a decrease of 375 from the 2,124 authorisations made in 2017–18.

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

Agency	Authorisations	
	17 / 18	18 / 19
ACCC	21	8
AFP	26	72
ASIC	105	39
Home Affairs	41	38
NT Police	1	1
NSW Police	1,235	1,206
QLD CCC	-	5
QLD Police	2	3
SA Police	4	-
TAS Police	678	374
WA Police[11]	11	3
TOTAL	**2,124**	**1,749**

[11] Correction for 17-18: WA Police's authorisations under section 179 have been amended from 0 to 11 due to a transposition error in the 2017-18 Annual Report. As such, the total figures have also been amended.

Prospective data – authorisations

Section 180 of the TIA Act provides that an authorised officer of a *criminal law-enforcement agency* may authorise the disclosure of prospective telecommunications data (data that comes into existence during the period for which the authorisation is in force) if they are satisfied it is reasonably necessary for the investigation of a serious offence or an offence against a law of the Commonwealth, a State or a Territory that is punishable by imprisonment for at least three years. Prospective data authorisations may also authorise the disclosure of historical data.

Section 186(1)(c) of the TIA Act provides that this report must set out the number of authorisations made under section 180 by agencies during the year.

This information is presented in Table 33. The table also outlines the number of days the authorisations were to be in force and how many days they were actually in force.

In 2018–19, 27,824 prospective authorisations were made by agencies under section 180, an increase of 3,877 on the 23,947 authorisations made in 2017–18.

Table 33: Prospective data authorisations – section 186(1)(c)

	Number of authorisations made		Days specified in force		Actual days in force		Authorisations discounted	
Agency	**17 / 18**	**18 / 19**	**17 / 18**	**18 / 19**	**17 / 18**	**18 / 19**	**17 / 18**	**18 / 19**
ACIC	1,401	1,279	41,809	39,671	30,475	29,938	28	35
ACLEI	182	88	8,056	3,960	7,068	3,748	24	-
AFP	3,701	4,707	144,571	195,466	124,850	108,218	416	302
ASIC	17	37	34	119	33	116	-	-
CCC (WA)	89	63	3,828	2,829	3,394	2,137	3	7
Home Affairs	264	225	614	523	604	504	-	3
IBAC	287	310	11,733	13,776	8,015	10,858	54	33
ICAC (NSW)	25	75	1,125	3,323	823	2,848	5	-
ICAC (SA)	31	25	1,318	962	1,157	841	31	6
LECC	64	65	2,825	2,925	2,466	2,449	-	7
NT Police	400	311	15,594	9,661	11,588	7,528	24	14
NSW CC	1,149	1,176	48,976	50,402	45,496	43,226	110	147
NSW Police	1,043	1,062	19,307	22,691	15,671	16,567	48	73
QLD CCC	203	210	8,753	8,540	7,303	6,351	35	8
QLD Police	3,430	4,252	146,478	185,008	100,823	138,986	394	342
SA Police	342	422	9,407	14,759	7,985	11,036	24	26
TAS Police	172	178	7,740	8,010	4,810	4,481	11	1
VIC Police	9,619	11,219	384,341	496,658	329,420	367,965	1,010	1,253
WA Police	1,528	2,120	54,928	75,812	38,533	74,877	130	224
TOTAL	**23,947**	**27,824**	**911,437**	**1,135,095**	**740,514**	**832,674**	**2,347**	**2,481**

Table 34 compares information about the average number of days prospective data authorisations under section 180 were specified to be in force and the average actual number of days they remained in force between 2018–19 and 2017–18.

Table 34: Average specified and actual time in force of prospective data authorisations

Agency	Average period specified		Average period actual	
	17 / 18	18 / 19	17 / 18	18 / 19
ACIC	30	31	22	24
ACLEI	44	45	45	43
AFP	39	42	38	25
ASIC	2	3	2	3
CCC (WA)	43	45	39	38
Home Affairs	2	2	2	2
IBAC	41	44	34	39
ICAC (NSW)	45	44	41	38
ICAC (SA)	43	38	37	44
LECC	44	45	39	42
NT Police	39	31	31	25
NSW CC	43	43	44	42
NSW Police	19	21	16	17
QLD CCC	43	41	43	31
QLD Police	43	44	33	36
SA Police	28	35	25	28
TAS Police	45	45	30	25
VIC Police	40	44	38	37
WA Police	36	36	28	39
AVERAGE	**35**	**36**	**31**	**30**

Data authorisations for foreign law enforcement

Foreign countries, the International Criminal Court and War Crimes Tribunals may request the AFP obtain telecommunications data to assist in an investigation or proceeding within their jurisdictions. The AFP may make authorisations to obtain telecommunications data for the purposes of disclosing that data to a requesting jurisdiction, or authorise the disclosure of telecommunications data the AFP has previously obtained.

Foreign requests for prospective telecommunications data must first be authorised by the Attorney-General under:

- section 15D of the *Mutual Assistance in Criminal Matters Act 1987;*
- section 78B of the *International Criminal Court Act 2002; or*
- section 34B of the *International War Crimes Tribunal Act 1995*.

Sections 186(1)(ca)-(cb) and 186(2) of the TIA Act provide that this report:

- must set out the number of authorisations made by the AFP under sections 180A, 180B, 180C and 180D during the year, and
- may also set out the number of disclosures made during the year and the names of each country to which disclosures were made.[12]

In 2018–19, the AFP made 62 authorisations under sections 180A, 180B, 180C and 180D of the TIA Act.

Following these authorisations, the AFP made 19 disclosures to foreign law enforcement agencies. Information was disclosed to the following countries: Belarus (1), Germany (2), India (4), Japan (1), New Zealand (2), Singapore (1), United Kingdom (1) and the United States of America (7).

[12] Correction for 2017-18: Since the publication of the 2017-18 TIA Act Annual Report, the AFP identified authorisations made during that reporting period under section 180(4) that had not been captured in their database. As such, amended figures for the reporting requirements under section 186(1)(ca)-(cb) for 17/18 are as follows: In 2017–18, the AFP made 69 authorisations under sections 180A, 180B, 180C and 180D of the TIA Act. Following these authorisations, the AFP made 13 disclosures to foreign law enforcement agencies. Information was disclosed to the following countries: Austria (1), Greece (2), India (1), Ireland (1), New Zealand (2), Singapore (1), Switzerland (1), the United Kingdom (1) and the United States of America (3).

Offences for which authorisations were made

Section 186(1)(e) of the TIA Act provides that this report must set out the offences and other matters for which authorised officers of each agency made authorisations under sections 178, 178A, 179 and 180. This information is presented in Tables 35, 36, 37 and 38.

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 35: Offences for which authorisations were made under section 178 to access existing data to enforce the criminal law – section 186(1)(e)[13]

Categories of offences	ACCC	ACIC	ACLEI	AFP	ASIC	CCC (WA)	Home Affairs	IBAC	ICAC (NSW)	ICAC (SA)	LECC	NT Police	NSW CC	NSW Police	QLD CCC	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Abduction	-	-	-	516	-	-		2	-	-	-	270	6	8213	-	1,345	295	612	1,044	2,176	**14,479**
ACIC Investigation	-	6,387	-	-	-	-	-	-	-	-	-	-	-	0	-	75	-	-	-	-	**6,462**
Acts - injury	-	-	-	144	-	-	-	1	-	-	3	52	-	4772	-	31	112	314	4,816	927	**11,172**
Bribery or corruption	-	-	393	161	-	122		423	31	219	305	2	6	0	79	-	211	-	70	596	**2,618**
Cartel offences	99	-	-	-	-	-	-	-	-	-	-	-	-	7	-	-	-	-	-	-	**106**
Conspire	-	-	-	76	18	-	-	-	-	-	-	1	-	138	-	1	2	262	636	67	**1,201**
Cybercrime	-	-	-	912	142	-	-	-	-	-	2	103	-	3428	-	777	6	17	957	388	**6,732**
Dangerous acts	-	-	-	93	-	-	-	21	-	-	-	110	-	985	-	1,270	339	12	2,186	42	**5,058**
Fraud	1	-	-	1,032	600	-	1,680	30	174	1	118	148	749	12526	310	750	371	377	8,092	1,498	**28,457**
Homicide	-	-	-	414	-	-	-	-	-	-	-	323	355	13922	-	1,572	874	631	5,833	1,684	**25,608**
Illicit drug offences	-	149	-	7,636	-	-	1,240	-	-	-	31	1,838	1,700	24833	586	4,234	1,472	3,358	19,150	6,450	**72,677**
Loss of life	-	-	-	25	-	-	-	-	-	-	-	-	-	588	-	400	5	-	9	-	**1,027**
Miscellaneous	-	-	-	212	1,222	-	18	11	-	-	-	119	19	3972	28	7,540	46	17	1,423	461	**15,088**
Justice procedures	-	-	-	317	11	-	22	40	93	-	-	7	1	663	-	-	49	77	999	153	**2,432**
Organised offences	-	-	-	620	-	-	-	-	-	-	-	5	-	974	-	-	3	-	-	503	**2,105**

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

Categories of offences	ACCC	ACIC	ACLEI	AFP	ASIC	CCC (WA)	Home Affairs	IBAC	ICAC (NSW)	ICAC (SA)	LECC	NT Police	NSW CC	NSW Police	QLD CCC	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Pecuniary penalty	-	-	-	26	-	-	-	-	-	-	-	-	-	625	-	-	-	17	-	-	**668**
Public revenue	-	-	-	6	-	-	-	-	-	-	-	-	-	0	-	-	-	-	-	-	**6**
People smuggling	-	-	-	260	-	-	21	-	-	-	-	-	-	0	-	-	-	-	-	1	**282**
Weapons	-	-	-	206	-	-	234	-	-	-	-	2	35	1593	6	12	174	56	3,383	466	**6,167**
Property damage	-	-	-	91	-	-	-	-	-	-	-	9	2	1133	-	-	249	-	2,496	119	**4,099**
Public order offences	-	-	-	14	-	-	-	-	-	-	-	-	-	76	-	28	9	36	-	44	**207**
Robbery	-	-	-	347	-	-	-	11	-	-	-	80	-	9289	-	1,131	350	228	8,771	1,872	**22,079**
Serious damage	-	-	-	16	-	-	-	-	-	-	-	54	1	499	-	467	69	128	4	475	**1,713**
Sexual assault	-	-	-	1,658	-	-	1	-	-	-	-	267	1	7605	-	1,089	418	266	4,798	1,150	**17,253**
Terrorism offences	-	-	-	1,367	-	-	8	-	-	-	-	2	448	695	-	-	28	1	977	147	**3,673**
Theft	-	-	-	466	-	-	59	-	-	-	-	99	-	5732	-	1,151	151	661	7,940	1,059	**17,318**
Traffic	-	-	-	44	-	-	-	-	-	-	-	8	-	873	-	183	2	28	967	70	**2,175**
Unlawful entry	-	-	-	159	-	-	-	-	-	-	-	46	-	2044	-	1,056	242	561	13,129	2,754	**19,991**
TOTAL	**100**	**6,536**	**393**	**16,818**	**1,993**	**122**	**3,283**	**539**	**298**	**220**	**459**	**3545**	**3,323**	**105,185**	**1,009**	**23,112**	**5,477**	**7,659**	**87,680**	**23,102**	**290,853**

Table 36: Offences against which authorisations were made under section 178A for access to existing data to locate a missing person – section 186(1)(e)[14]

Categories of offences	AFP	NT Police	NSW Police	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Abduction	-	-	30	3	-	-	-	-	**33**
ACC Investigation	-	-	-	-	-	-	-	-	**-**
Acts – injury	-	-	12	-	-	-	-	-	**12**
Bribery or corruption	-	-	-	-	-	-	-	-	**-**
Cartel offences	-	-	2	-	-	-	-	-	**2**
Conspire	-	-	1	-	-	-	-	-	**1**
Cybercrime	-	-	-	-	-	-	-	-	**-**
Dangerous acts	-	-	-	-	-	-	-	-	**-**
Fraud	-	-	-	-	-	-	-	-	**-**
Homicide	-	-	8	35	-	-	-	-	**43**
Illicit drug offences	-	-	-	-	-	-	-	-	**-**
Loss of life	-	-	39	-	-	-	-	-	**39**
Miscellaneous	-	-	68	31	-	-	-	-	**99**
Justice procedures	-	-	1	-	-	-	-	-	**1**
Organised offences	-	-	-	-	-	-	-	-	**-**
Pecuniary penalty	-	-	-	-	-	-	-	-	**-**

[14] Section 178A authorisations are not required to be connected to an underlying offence, only for the purposes of locating a missing person.

Categories of offences	AFP	NT Police	NSW Police	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Public revenue	-	-	-	-	-	-	-	-	**-**
People smuggling	-	-	-	-	-	-	-	-	**-**
Weapons	-	-	-	-	-	-	-	-	**-**
Property damage	-	-	-	-	-	-	-	-	**-**
Public order offences	-	-	-	-	-	-	-	-	**-**
Robbery	-	-	1	2	-	-	-	-	**3**
Serious damage	-	-	-	1	-	-	-	-	**1**
Sexual assault	-	-	2	-	-	-	-	-	**2**
Terrorism offences	-	-	-	-	-	-	-	-	**-**
Theft	-	-	-	-	-	-	-	-	**-**
Traffic	-	-	-	-	-	-	-	-	**-**
Unlawful entry	-	-	-	-	-	-	-	-	**-**
No offence attached to s178A authorisation	194	31	1,064	127	79	168	447	243	**2,353**
TOTAL	**194**	**31**	**1,228**	**199**	**79**	**168**	**447**	**243**	**2,589**

Table 37: Offences against which authorisations were made under section 179 for access to existing data for the enforcement of a law imposing a pecuniary penalty or protection of the public revenue – section 186(1)(e)

Categories of offences	ACCC	AFP	ASIC	Home Affairs	NT Police	NSW Police	QLD CCC	QLD Police	TAS Police	WA Police	TOTAL
Abduction	-	3	-	-	-	33	-	-	59	-	**95**
ACC Investigation	-	-	-	-	-	-	-	-	-	-	**-**
Acts – injury	-	-	-	-	-	9	-	-	25	-	**34**
Bribery or corruption	-	-	-	-	-	-	-	-	-	-	**-**
Cartel offences	-	-	-	-	-	-	-	-	-	-	**-**
Conspire	-	44	2	-	-	-	-	-	-	-	**46**
Cybercrime	-	-	-	-	-	6	-	-	12	-	**18**
Dangerous acts	-	-	-	-	-	10	-	-	-	-	**10**
Fraud	-	5	34	6	-	44	5	-	1	-	**95**
Homicide	-	-	-	-	-	24	-	-	-	-	**24**
Illicit drug offences	-	7	-	3	-	49	-	1	1	-	**61**
Loss of life	-	-	-	-	-	1	-	-	-	-	**1**
Miscellaneous	-	2	18	-	-	72	-	2	12	-	**106**
Justice procedures	-	1	2	-	-	8	-	-	56	-	**67**
Organised offences	-	4	-	-	-	268	-	-	1	-	**273**
Pecuniary penalty	8	4	-	19	-	59	-	-	25	3	**118**

Categories of offences	ACCC	AFP	ASIC	Home Affairs	NT Police	NSW Police	QLD CCC	QLD Police	TAS Police	WA Police	TOTAL
Public revenue	-	2	-	-	-	-	-	-	-	-	**2**
People smuggling	-	-	-	-	-	-	-	-	-	-	**-**
Weapons	-	-	-	9	-	-	-	-	21	-	**30**
Property damage	-	-	-	-	-	5	-	-	-	-	**5**
Public order offences	-	-	-	-	-	-	-	-	3	-	**3**
Robbery	-	-	-	-	-	390	-	-	-	-	**390**
Serious damage	-	-	-	-	-	-	-	-	7	-	**7**
Sexual assault	-	-	-	-	-	31	-	-	5	-	**36**
Terrorism offences	-	1	-	-	-	14	-	-	-	-	**15**
Theft	-	-	-	1	-	32	-	-	99	-	**132**
Traffic	-	-	-	-	1	38	-	-	-	-	**39**
Unlawful entry	-	-	-	-	-	127	-	-	29	-	**156**
TOTAL	**8**	**73**	**56**	**38**	**1**	**1,220**	**5**	**3**	**356**	**3**	**1,763**

Table 38: Offences against which authorisations were made under section 180 for access to specified information or documents that come into existence during the period for which an authorisation is in force – section 186(1)(e)

Categories of offences	ACIC	ACLEI	AFP	ASIC	CCC (WA)	Home Affairs	IBAC	ICAC (NSW)	ICAC (SA)	LECC	NT Police	NSW CC	NSW Police	QLD CCC	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Abduction	-	-	64	-	-	-	-	-	-	-	10	2	53	-	57	19	15	338	39	**597**
ACC Investigation	1,265	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**1,265**
Acts – injury	-	-	17	-	-	-	-	-	-	-	4	-	98	-	153	17	-	871	67	**1,227**
Bribery or corruption	-	88	28	-	63	-	266	2	25	52	-	-	-	93	-	-	-	32	-	**649**
Cartel offences	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**-**
Conspire	-	-	27	-	-	-	-	-	-	-	-	-	-	-	5	1	4	27	58	**122**
Cybercrime	-	-	154	13	-	-	-	-	-	-	-	-	2	-	-	-	1	19	-	**189**
Dangerous acts	-	-	2	-	-	-	18	-	-	-	2	-	6	-	18	13	-	328	5	**392**
Fraud	-	-	191	37	-	151	5	69	-	5	2	257	32	6	153	7	-	615	25	**1,555**
Homicide	-	-	46	-	-	-	-	-	-	-	7	24	50	-	329	39	17	495	33	**1,040**
Illicit drug offences	14	-	2,343	-	-	32	-	-	-	7	260	640	435	111	277	217	104	3,470	1,208	**9,118**
Loss of life	-	-	5	-	-	-	-	-	-	-	-	-	27	-	18	3	-	47	-	**100**
Miscellaneous	-	-	20	-	-	-	-	-	-	1	2	5	52	-	54	3	-	-	28	**165**
Justice procedures	-	-	104	-	-	-	21	4	-	-	-	2	5	-	-	3	-	16	4	**159**
Organised offences	-	-	1,228	-	-	-	-	-	-	-	-	-	17	-	31	3	-	2	-	**1,281**
Pecuniary penalty	-	-	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	-	**1**

Categories of offences	ACIC	ACLEI	AFP	ASIC	CCC (WA)	Home Affairs	IBAC	ICAC (NSW)	ICAC (SA)	LECC	NT Police	NSW CC	NSW Police	QLD CCC	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Public revenue	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**-**
People smuggling	-	-	35	-	-	-	-	-	-	-	-	-	-	-		-	-	-	-	**35**
Weapons	-	-	74	-	-	32	-	-	-	-	-	19	65	-	59	25	5	509	51	**839**
Property damage	-	-	20	-	-	-	-	-	-	-	-	-	9	-	1	-	4	-	-	**34**
Public order offences	-	-	1	-	-	-	-	-	-	-	-	-	1	-	-	-	-	1	1	**4**
Robbery	-	-	50	-	-	-	-	-	-	-	5	-	100	-	220	34	4	976	132	**1,521**
Serious damage	-	-	2	-	-	-	-	-	-	-	2	-	6	-	38	-	-	209	14	**271**
Sexual assault	-	-	75	-	-	-	-	-	-	-	12	-	13	-	43	5	1	571	30	**750**
Terrorism offences	-	-	72	-	-	-	-	-	-	-	-	227	2	-	5	-	-	43	1	**350**
Theft	-	-	97	-	-	10	-	-	-	-	4	-	59	-	67	10	3	1,160	58	**1,468**
Traffic	-	-	2	-	-	-	-	-	-	-	-	-	1	-	-	2	-	33	11	**49**
Unlawful entry	-	-	47	-	-	-	-	-	-	-	1	-	28	-	224	21	20	1,457	355	**2,153**
TOTAL	**1,279**	**88**	**4,704**	**50**	**63**	**225**	**310**	**75**	**25**	**65**	**311**	**1,176**	**1,062**	**210**	**1,752**	**422**	**178**	**11,219**	**2,120**	**25,334**

Age of data under disclosure

Sections 186(1)(f) and 186(1C) of the TIA Act provide that this report must set out the lengths of time for which information or documents covered by historical data authorisations had been held by a service provider before the authorisations for that information were made.

Table 39 provides this information. The statistics are split into successive periods of three 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.

In 2018–19, 85 per cent of authorisations were for data 0–3 months old. This includes 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] which 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 reporting period, 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 39: Periods which retained data was held by carrier before authorised disclosure – section 186(1)(f)

Agency	Age of 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	8	17	13	12	4	5	4	3	42	**108**
ACIC	5,471	748	144	55	51	22	5	1	39	**6,536**
ACLEI	182	17	42	20	4	9	6	8	105	**393**
AFP	12,496	1,689	630	821	323	146	88	175	760	**17,128**
ASIC	1,549	70	90	26	27	10	6	8	39	**1,825**
CCC (WA)	116	2	2	1	-	1	-	-	-	**122**
Home Affairs	2,670	405	178	106	72	20	16	9	70	**3,546**
IBAC	439	10	7	12	7	5	8	12	39	**539**
ICAC (NSW)	100	22	14	6	22	17	11	10	96	**298**
ICAC (SA)	39	54	22	30	33	8	3	3	28	**220**
LECC	314	41	22	28	8	8	-	1	37	**459**
NT Police	3,267	67	23	34	18	12	15	8	52	**3,496**
NSW CC	2,556	170	67	97	87	43	19	51	233	**3,323**
NSW Police	98,125	3,637	1,739	1,493	604	316	246	380	1,093	**107,633**
QLD CCC	607	152	75	52	27	33	8	3	57	**1,014**
QLD Police	19,709	1,561	888	556	320	204	114	86	454	**23,892**
SA Police	3,496	673	418	237	103	72	92	59	445	**5,595**
TAS Police	7,632	304	97	56	22	42	12	12	113	**8,290**
VIC Police	77,958	4,003	1,784	1,168	578	425	352	213	1,281	**87,762**
WA Police	17,095	1,936	1,107	629	493	312	270	146	1,360	**23,348**
TOTAL	**253,829**	**15,578**	**7,362**	**5,439**	**2,803**	**1,710**	**1,275**	**1,188**	**6,343**	**295,527**

Types of retained data

Sections 186(1)(g)-(h) of the TIA Act provide that this report must set out the number of occasions during the reporting period that agencies made authorisations for retained data which included information from the data subsets identified in section 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 40: Types of retained data disclosed in authorisations – sections 186(1)(g) and 186(1)(h)

Agency	Item 1: subscriber data	Items 2 – 6: traffic data	TOTAL
ACCC	60	48	**108**
ACIC	4,082	2,454	**6,536**
ACLEI	226	167	**393**
AFP	12,687	4,305	**16,992**
ASIC	1,569	256	**1,825**
CCC (WA)	83	102	**185**
Home Affairs	2,513	877	**3,390**
IBAC	415	140	**555**
ICAC (NSW)	169	129	**298**
ICAC (SA)	128	92	**220**
LECC	318	141	**459**
NT Police	3,008	667	**3,675**
NSW CC	2,292	1,554	**3,846**
NSW Police	76,736	30,897	**107,633**
QLD CCC	750	264	**1,014**
QLD Police	18,999	4,896	**23,895**
SA Police	3,677	1,918	**5,595**
TAS Police	7,172	1,129	**8,301**
VIC Police	65,069	23,058	**88,127**
WA Police	18,695	4,653	**23,348**
TOTAL	**218,648**	**77,747**	**296,395**

[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.

Sections 186(1)(i)-(j) of the TIA Act provide that this report must set out the number of JIWs issued to agencies during the year and the number of authorisations made under JIWs issued to those agencies.

Tables 41 and 42 present this information. In 2018–19, 20 historical data authorisations were made under six JIWs issued to the AFP for the enforcement of the criminal law.

Table 41: Journalist information warrants issued – section 186(1)(j)

Agency	Warrants Issued	
	17 / 18	18 / 19
AFP	2	6

Table 42: Number of authorisations made under journalist information warrants – section 186(1)(i)

Agency	Authorisations made									
	17 / 18					18 / 19				
	s178	s78A	s179	s180	TOTAL	s178	s178A	s179	s180	TOTAL
AFP	58	-	-	-	**58**	20	-	-	-	**20**

Industry estimated cost of implementing data retention

Since 13 October 2015, carriers and service providers have been required to comply with the data retention obligations in Part 5-1A of the TIA Act. Section 187P of the TIA Act provides that this report must include information about the costs to service providers of complying with the data retention scheme and the use of data retention implementation plans.

Information collected from industry by the Australian Communications and Media Authority (ACMA), shows the cost of complying with the data retention obligations for the five financial years commencing July 2014 and ending June 2019 (set out in Table 43).

Table 43 further sets out the costs recovered from criminal law-enforcement agencies for the purpose of complying with their data retention obligations.

Table 43: Industry Capital Costs of data retention – section 187P(1A)

Financial year	Data retention compliance cost (GST inclusive) (*exclusive of data retention industry grants*)	Costs recovered from criminal law-enforcement agencies (GST inclusive)
2014–15	$11,972,288.15	$7,316,341.41
2015–16	$44,426,132.06	$9,412,132.06
2016–17	$119,793,739.83	$9,829,783.17
2017–18	$35,355,577.00	$12,515,681.00
2018–19	$17,453,069.00	$7,443,035.00
TOTAL	**$229,000,806.04**	**$46,516,972.64**

The Data Retention Industry Grants Programme closed on 23 February 2016 with the last funding provided during the 2017–18 reporting period. As such, there was no funding provided under the Data Retention Industry Grants Programme in 2018–19.

CHAPTER 4 – INDUSTRY ASSISTANCE

The Assistance and Access Act established an industry assistance framework at Part 15 of the Telecommunications Act to provide a structure through which Australian agencies and the communications industry can work together to address technological obstacles to investigations into serious crime and national security threats. The industry assistance framework statistics in this chapter reflect this framework being available for use by law enforcement agencies between 9 December 2018 and 30 June 2019.

Requests and notices

Part 15 of the Telecommunications Act establishes a graduated approach for agencies to receive assistance from industry by establishing three powers:

- **Technical Assistance Request (TAR):** Agencies can request voluntary help from designated communications providers[17] where they are willing and able to give assistance.
- **Technical Assistance Notice (TAN):** Agencies can compel designated communications providers to give assistance where they already have the technical capability to do so.
- **Technical Capability Notice (TCN):** Agencies can require providers build limited capabilities to help law enforcement and security authorities. The Attorney-General and the Minister for Communications must both agree to give a designated communications provider a TCN.

Table 44: Eligible agencies under Part 15 of the Telecommunications Act

Agency	Industry assistance powers available to agencies		
	TAR	TAN	TCN
Interception Agencies[18]	✓	✓	✓
ASD	✓	✗	✗
ASIO	✓	✓	✓
ASIS	✓	✗	✗

Definition

'Interception agency' in Part 15 of the Telecommunications Act means:

- the Australian Federal Police;
- the Australian Criminal Intelligence Commission; and
- the Police Force of a State or the Northern Territory.

[17] Categories of designated communications providers and their eligible activities are at Appendix G
[18] In contrast to the TIA Act, this does not include anti-corruption and integrity commissions.

The industry assistance framework provides that:

- any assistance or capability requested must be reasonable, proportionate, practicable and technically feasible;
- assistance to law enforcement must be related to investigating serious Australian offences or assisting the enforcement of serious foreign offences, or safeguarding national security;
- providers may be asked to use or build capabilities that can provide targeted access to data where this does not remove electronic protection or jeopardise the information security of general users.

Definition

'Serious Australian offence' is an offence against a law of the Commonwealth, a State or a Territory that is punishable by a maximum term of imprisonment of three years or more or for life.

'Serious foreign offences' are an offence against a law in force in a foreign country that is punishable by a maximum term of imprisonment of three years or more or for life.

The framework contains numerous limitations and safeguards including:

- prohibiting assistance that creates 'systemic weaknesses' in encrypted devices and communication systems. This includes a prohibition on requesting or requiring providers to refrain from fixing vulnerabilities or making their systems more secure, build a decryption capability, or reduce the broader security of their systems;
- to see the content of personal communications or intercept communications, agencies must still obtain the necessary warrant or authorisation under the relevant law of the Commonwealth, States or Territories (such as a warrant under the TIA Act);
- assistance cannot compel providers to build a capability to remove electronic protection or extend existing data retention and interception obligations to new providers.

Definition

'Systemic weakness' means a weakness that affects a whole class of technology, but does not include a weakness that is selectively introduced to one or more target technologies that are connected with a particular person. For this purpose, it is immaterial whether the person can be identified.

Use of industry assistance

Sections 317ZS(1)(a)-(c) of the Telecommunications Act provide that this report must set out the number of TARs and TANs given by the chief officers of interception agencies during the year, and the number of TCNs given during the year that were directed towards ensuring designated communications providers were capable of giving help to interception agencies.

This information is presented in Table 45. In 2018–19, seven TARs were given by interception agencies to designated communications providers. Five were given by the AFP, and two were given by NSW Police. No TANs or TCNs were given by interception agencies.

Table 45: Number of Technical Assistance Requests, Technical Assistance Notices, and Technical Capability Notices given between 9 December 2018 and 30 June 2019 – sections 317ZS(1)(a)-(b) and 317ZS(c)(i)-(ii) of the Telecommunications Act

Agency	Requests or notices given			
	Technical Assistance Request	Technical Assistance Notice	Technical Capability Notice	TOTAL
AFP	5	-	-	**5**
NSW Police	2	-	-	**2**
TOTAL	**7**	**-**	**-**	**7**

Offences enforced through industry assistance

Section 317ZS(1)(d) of the Telecommunications Act provides that if any TARs, TANs or TCNs given during the year related to one or more kinds of serious Australian offences—this report must set out those kinds of serious Australian offences.

Table 46 provides this information for the 2018–19 period. The total number of offences is larger than the number of requests and notices given, as a single request or notice can relate to the enforcement of more than one serious Australian offence.

The offence categories listed in the table are based on the Australian and New Zealand Standard Offence Classification, published by the Australian Bureau of Statistics. The Department of Home Affairs has added additional categories to better reflect the offence categories for which requests and notices may be given.[19]

[19] Appendix F contains a description of each of the categories of offences.

Table 46: Kinds of serious Australian offences enforced through technical assistance requests – section 317ZS(1)(d) of the *Telecommunications Act 1997*

Categories of offences	AFP	NSW Police	TOTAL
Abduction offences	-	-	**-**
ACIC Investigation	-	-	**-**
Acts intended to cause injury	-	-	**-**
Bribery or corruption	-	-	**-**
Cartel offences	-	-	**-**
Conspire/aid/abet offences	-	-	**-**
Cybercrime offences	6	-	**6**
Dangerous acts endangering a person	-	-	**-**
Fraud and deception	-	-	**-**
Homicide	-	1	**1**
Illicit drug offences	-	1	**1**
Loss of life	-	-	**-**
Justice procedures	-	-	**-**
Organised offences	2	-	**2**
People smuggling	-	-	**-**
Weapons offences	-	-	**-**
Property damage	-	-	**-**
Public order offences	-	-	**-**
Robbery	-	-	**-**
Serious damage	-	-	**-**
Sexual assault	-	-	**-**
Telecommunications offences	5	-	**5**
Terrorism offences	-	-	**-**
Theft	1	-	**1**
Traffic offences	-	-	**-**
Unlawful entry	-	-	**-**
TOTAL	**14**	**2**	**16**

Oversight of industry assistance powers

Use of the industry assistance framework by agencies is subject to independent oversight by either the Inspector-General of Intelligence and Security, the Commonwealth Ombudsman or State and Territory oversight bodies.

The Inspector-General of Intelligence and Security or the Commonwealth Ombudsman (as relevant) must be notified whenever a notice for assistance is given, varied, extended or revoked. When an agency gives a notice, they must notify the company of their right to complain to the relevant body. Both the Commonwealth Ombudsman and the Inspector-General of Intelligence and Security have the authority to inspect the use of these powers by relevant agencies at any time. These bodies may make reports to Parliament on the outcome of their inspections.

The Commonwealth Ombudsman may also, during their inspections under the TIA Act, inspect agencies' records of TARs, TANs and TCNs when the measures have been used in connection with an interception warrant, a stored communications warrant or a telecommunications data authorisation. As the new industry assistance measures complement these existing TIA Act powers, this ensures the Commonwealth Ombudsman can oversight their joint use.

Compulsory powers carry additional oversight measures to ensure they are used appropriately. Where a State or Territory law enforcement agency issues a notice to compel technical assistance through a TAN, it must first be reviewed by the Australian Federal Police Commissioner.

TCNs may only be issued by the Attorney-General, with the approval of the Minister for Communications. This creates a double-lock approval process to ensure the assistance sought has been thoroughly scrutinised and is reasonable, proportionate, practicable and technically feasible.

If requested to by a company, the Attorney-General must refer any proposed requirement to build a capability to an independent assessment panel consisting of a retired senior judge and a technical expert. This panel must consider whether proposed requirements will inadvertently create a backdoor. Further, any decision to compel assistance may be challenged through judicial review proceedings.

Designated communications providers may make a complaint to the relevant oversight body for the agency that issued the request or notice. In the case of ASIO, ASD and ASIS this is the Inspector-General of Intelligence and Security. In the case of interception agencies this is the Commonwealth Ombudsman. Additionally, in the case of State and Northern Territory Police, providers are advised that they may contact the inspecting authority of the relevant State or the Northern Territory to complain about an assistance instrument they have been issued. [20]

[20] Further information on the Assistance and Access Act including detailed administrative guidance can be found on the website of the Department of Home Affairs, at www.homeaffairs.gov.au.

CHAPTER 5 – FURTHER INFORMATION

For further information about the *Telecommunications (Interception and Access) Act 1979* and Part 15 of the *Telecommunications Act 1997*, please contact the Department of Home Affairs:

National Security Policy Branch

Department of Home Affairs

PO Box 25

BELCONNEN ACT 2616

(02) 6264 1111

More information about telecommunications interception and access and telecommunications data access can be found at <www.homeaffairs.gov.au>

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

APPENDIX A – LISTS OF TABLES AND 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 Criminal Intelligence Commission	Not applicable
Australian Federal Police	Not applicable
Crime and Corruption 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
Law Enforcement Conduct Commission	11 May 2017
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
ACIC	Australian Criminal Intelligence Commission
ACCC	Australian Competition and Consumer Commission
ACLEI	Australian Commission for Law Enforcement Integrity
AFP	Australian Federal Police
AGD	Attorney-General's Department
ASD	Australian Signals Directorate
ASIC	Australian Securities and Investments Commission
ASIO	Australian Security Intelligence Organisation
ASIS	Australian Secret Intelligence Service
Assistance and Access Act	*Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*
CCC (WA)	Corruption and Crime Commission (Western Australia)
Home Affairs	Department of Home Affairs
IBAC	Independent Broad-based Anti-corruption Commission (Victoria)
LECC	Law Enforcement Conduct Commission
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
PIM	Public Interest Monitor
PJCIS	Parliamentary Joint Committee on Intelligence and Security
QLD CCC	Queensland Corruption and Crime Commission
QLD Police	Queensland Police Service
ICAC (SA)	Independent Commissioner Against Corruption (South Australia)
SA Police	South Australia Police
TAR	Technical Assistance Request
TAN	Technical Assistance Notice
TCN	Technical Capability Notice
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 UNDER THE TIA ACT

Serious offence category	Offences covered
ACIC special investigation	TIA Act, s 5D(1)(f)
Administration of justice/government offences	TIA Act, s 5D(8)(a) and (b)
Assist escape punishment/dispose of proceeds	TIA Act, s 5D(7)
Bribery or corruption; offences	TIA Act, s 5D(2)(vii);
Cartel offences	TIA Act, s 5D(5B)
Child pornography offences	TIA Act, s 5D(3B)
Conspire/aid/abet serious offence	TIA Act, s 5D(6)
Cybercrime offences	TIA Act, s 5D(5)
Espionage and foreign interference offences	TIA Act, s 5D(1)(e)(ic),(id),(ie),(if),(ig),(vii) and (viii)
Kidnapping	TIA Act, s 5D(1)(b)
Loss of life or personal injury	TIA Act, s 5D(2)(b)(i) and (ii)
Money laundering	TIA Act, s 5D(4)
Murder	TIA Act, s 5D(1)(a)
Offences involving planning and organisation	TIA Act, s 5D(3)
Organised offences and/or criminal organisations	TIA Act, s 5D(3AA), s5D(8A) and (9)
People smuggling and related	TIA Act, s 5D(3A)
Serious damage to property and/or serious arson	TIA Act, s 5D(2)(b)(iii) and (iiia)
Serious drug offences and/or trafficking	TIA Act, s 5D(5A); s 5D(2)(b)(iv); s 5D(1)(c)
Serious fraud	TIA Act, s 5D(2)(v)
Serious loss of revenue	TIA Act, s 5D(2)(vi)
Telecommunications offences	TIA Act, s 5D(5)(a)
Terrorism financing offences	TIA Act, s 5D(1)(e)(iv)
Terrorism offences	TIA Act, s 5D(1)(d), s 5D(1)(e)(i),(ib),(ii),(iii) and (v)

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: (a) any information that is one or both of the following: i) any name or address information; ii) any other information for identification purposes; relating to the relevant service, being information used by the service provider for the purposes of identifying the subscriber of the relevant service; (b) any information relating to any contract, agreement or arrangement relating to the relevant account, service or device; (c) any information that is one or both of the following: (i) billing or payment information; (ii) contact information; relating to the relevant service, being information used by the service provider in relation to the relevant service; (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; (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. This category also includes details about services attached to the 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. This category further includes billing and payment information. 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. 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. 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. Service providers are not required to collect and retain passwords, PINs, secret questions or token codes, which are used for authentication purposes.

	Item	Description of information	Explanation
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: • the phone number, IMSI, IMEI from which a call or SMS was made • 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) • the IP address and port number allocated to the subscriber or device connected to the internet at the time of the communication, or • any other service or device identifier known to the provider that uniquely identifies the source of the communication. 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: a) has been sent; or b) has been forwarded, routed or transferred, or attempted to be forwarded, routed or transferred.	Section 187A(4)(b) puts beyond doubt that service providers are not required to keep information about subscribers' web browsing history. The destination of a communication is the recipient. Identifiers for the destination of a communication may include, but are not limited to: • The phone number that received a call or SMS. • Identifying details (such as username, address, or number) of the account, service, or device which receives a text, voice, or multi-media communication (example include email, VoIP, instant message or video communication). • The IP address allocated to a subscriber or device connected to the internet at the time of receipt of the communication. • Any other service or device identifier known to the provider that uniquely identifies the destination of the communication. 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. 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.
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): a) the start of the communication b) the end of the communication c) the connection to the relevant service, and d) the disconnection from the relevant service.	For phone calls this is simply the time a call started and ended. 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.

	Item	Description of information	Explanation
5.	**The type of communication and relevant service used in connection with a communication**	The following: a) the type of communication; Examples: Voice, SMS, email, chat, forum, social media. b) the type of the relevant service; Examples: ADSL, Wi-Fi, VoIP, cable, GPRS, VoLTE, LTE. c) the features of the relevant service that were, or would have been, used by or enable for the communication. 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). The type of the relevant service (see 5(b) at left) provides more technical detail about the service. For example, for a mobile messaging service, whether it is an SMS or MMS. 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. Note: This item will only apply to the service provider operating the relevant service: see section 187A(4)(c).
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: a) the location of the equipment or line at the start of the communication; b) the location of the equipment or line at the end of the communication. 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. 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. Section 187(4)(e) of the Act 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. 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 location 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 related offences
Unlawful entry	Unlawful entry with intent / burglary, break and enter

APPENDIX G – DESIGNATED COMMUNICATIONS PROVIDERS

Designated communications providers and eligible activities (section 317C of the Telecommunications Act)		
Item	**A person is a designated communications provider if…**	**…and the eligible activities of the person are…**
1	the person is a carrier or carriage service provider	(a) the operation by the person of telecommunications networks, or facilities, in Australia; or (b) the supply by the person of listed carriage services
2	the person is a carriage service intermediary who arranges for the supply by a carriage service provider of listed carriage services	(a) the arranging by the person for the supply by the carriage service provider of listed carriage services; or (b) the operation by the carriage service provider of telecommunications networks, or facilities, in Australia; or (c) the supply by the carriage service provider of listed carriage services
3	the person provides a service that facilitates, or is ancillary or incidental to, the supply of a listed carriage service	the provision by the person of a service that facilitates, or is ancillary or incidental to, the supply of a listed carriage service
4	the person provides an electronic service that has one or more end-users in Australia	the provision by the person of an electronic service that has one or more end-users in Australia
5	the person provides a service that facilitates, or is ancillary or incidental to, the provision of an electronic service that has one or more end-users in Australia	the provision by the person of a service that facilitates, or is ancillary or incidental to, the provision of an electronic service that has one or more end-users in Australia
6	the person develops, supplies or updates software used, for use, or likely to be used, in connection with: (a) a listed carriage service; or (b) an electronic service that has one or more end-users in Australia	(a) the development by the person of any such software; or (b) the supply by the person of any such software; or (c) the updating by the person of any such software
7	the person manufactures, supplies, installs, maintains or operates a facility	(a) the manufacture by the person of a facility for use, or likely to be used, in Australia; or (b) the supply by the person of a facility for use, or likely to be used, in Australia; or (c) the installation by the person of a facility in Australia; or (d) the maintenance by the person of a facility in Australia; or (e) the operation by the person of a facility in Australia

Designated communications providers and eligible activities (section 317C of the Telecommunications Act)		
8	the person manufactures or supplies components for use, or likely to be used, in the manufacture of a facility for use, or likely to be used, in Australia	(a) the manufacture by the person of any such components; or (b) the supply by the person of any such components
9	the person connects a facility to a telecommunications network in Australia	the connection by the person of a facility to a telecommunications network in Australia
10	the person manufactures or supplies customer equipment for use, or likely to be used, in Australia	(a) the manufacture by the person of any such customer equipment; or (b) the supply by the person of any such customer equipment
11	the person manufactures or supplies components for use, or likely to be used, in the manufacture of customer equipment for use, or likely to be used, in Australia	(a) the manufacture by the person of any such components; or (b) the supply by the person of any such components
12	the person: (a) installs or maintains customer equipment in Australia; and (b) does so otherwise than in the capacity of end-user of the equipment	(a) any such installation by the person of customer equipment; or (b) any such maintenance by the person of customer equipment
13	the person: (a) connects customer equipment to a telecommunications network in Australia; and (b) does so otherwise than in the capacity of end-user of the equipment	any such connection by the person of customer equipment to a telecommunications network in Australia
14	the person is a constitutional corporation who: (a) manufactures; or (b) supplies; or (c) installs; or (d) maintains; data processing devices	(a) the manufacture by the person of data processing devices for use, or likely to be used, in Australia; or (b) the supply by the person of data processing devices for use, or likely to be used, in Australia; or (c) the installation by the person of data processing devices in Australia; or (d) the maintenance by the person of data processing devices in Australia

	Designated communications providers and eligible activities (section 317C of the Telecommunications Act)	
15	the person is a constitutional corporation who: (a) develops; or (b) supplies; or (c) updates; software that is capable of being installed on a computer, or other equipment, that is, or is likely to be, connected to a telecommunications network in Australia	(a) the development by the person of any such software; or (b) the supply by the person of any such software; or (c) the updating by the person of any such software

NOTES