Australian Government

Department of Home Affairs

Telecommunications (Interception and Access) Act 1979

Annual Report 2019–20

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 2019–20

Contents

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)
ICAC (NSW)	Independent Commission Against Corruption (New South Wales)
ICAC (SA)	Independent Commissioner Against Corruption (South Australia)
INSLM	Independent National Security Legislation Monitor
LECC	Law Enforcement Conduct Commission
NSW CC	New South Wales Crime Commission
NSW Police	New South Wales Police Force
NT Police	Northern Territory Police Force
PJCIS	Parliamentary Joint Committee on Intelligence and Security
QLD CCC	Queensland Corruption and Crime Commission
QLD Police	Queensland Police Service
SA Police	South Australia Police
TAN	Technical Assistance Notice
TAR	Technical Assistance Request
TAS Police	Tasmania Police
TCN	Technical Capability Notice
Telecommunications Act	*Telecommunications Act 1997*
TIA Act	*Telecommunications (Interception and Access) Act 1979*
VIC Police	Victoria Police
WA Police	Western Australia Police Force

EXECUTIVE SUMMARY

The 2019–20 Annual Report for the *Telecommunications (Interception and Access) Act 1979* (TIA Act) sets out the extent to and circumstances in which eligible Commonwealth, State and Territory government law enforcement agencies have used the powers available under the TIA Act between 1 July 2019–30 June 2020.

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 information held by communications providers to investigate criminal offences and other activities that threaten the safety and security of Australians. The access that may be sought under the TIA Act includes access to telecommunications data, stored communications, and the interception of communications in real time. Each of the powers available under the TIA Act are explained below. Law enforcement agencies' use of warrants and authorisations related to these powers is independently overseen by the Commonwealth Ombudsman and equivalent state bodies.

Legislative reforms

Combatting Child Sexual Exploitation Legislation Amendment Act 2019

The *Combatting Child Sexual Exploitation Legislation Amendment Act 2019* amended paragraph 5D(3B)(a) of the TIA Act to provide that the possession of child-like sex dolls constitutes a serious offence for which a telecommunications interception warrant may be issued. This Act also amended the TIA Act to repeal the definition of, and references to, 'child pornography' and substituted it with 'child abuse material' to provide a more comprehensive definition and ensure consistency across Commonwealth legislation when referring to all explicit materials involving minors.

Australian Crime Commission Amendment (Special Operations and Special Investigations) Act 2019

The *Australian Crime Commission Amendment (Special Operations and Special Investigations) Act 2019* amended the TIA Act to repeal the definition of 'ACC operation/investigation' in subsection 5(1) and replace it with 'special ACC investigation'. This is to ensure that the TIA Act accurately reflects the *Australian Crime Commission Act 2002*.

Telecommunications (Interception and Access) Amendment (Assistance and Access Amendments Review) Act 2019

The *Telecommunications (Interception and Access) Amendment (Assistance and Access Amendments Review) Act 2019* amended the TIA Act to extend the date for finalisation of the Parliamentary Joint Committee on Intelligence and Security's (PJCIS) third review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (Assistance and Access Act) from 30 June 2020 to 30 September 2020. This

implemented a recommendation made by the PJCIS to allow the committee adequate time to consider the findings of the then Independent National Security Legislation Monitor (INSLM), Dr James Renwick CSC SC, following his review of the Assistance and Access Act.

Financial Sector Reform (Hayne Royal Commission Response—Stronger Regulators (2019 Measures)) Act 2020

The *Financial Sector Reform (Hayne Royal Commission Response—Stronger Regulators (2019 Measures)) Act 2020* amended the TIA Act to allow ASIC to receive and use intercepted information for its own investigations and prosecutions of serious offences. This legislative reform does not allow ASIC to intercept information itself, but rather allows ASIC to receive and use information already intercepted by other agencies.

Policy developments

During the 2019–20 reporting period, there were two reviews relating to the Assistance and Access Act and one review relating to the TIA Act that either commenced, continued, or were completed.

Review of the mandatory data retention regime

On 2 April 2019, the PJCIS commenced a review of the mandatory retention regime as required by section 187N of the TIA Act. The *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Data Retention Act) introduced a new legislative framework at Part 5-1 of the TIA Act. The framework 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 concluded its review and handed down its report in October 2020. The report considers the ongoing effectiveness of the scheme, taking into account changes in the use of technology since the scheme was introduced. The report also reassessed the appropriateness of the types of datasets being retained and the retention period, security requirements in relation to data stored under the regime, and oversight of the regime. The report makes 22 recommendations and at the time this report was provided to the Minister for Home Affairs, the Government was considering the PJCIS' recommendations.

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

On 27 March 2019, the PJCIS referred the Assistance and Access Act to the INSLM, Dr James Renwick CSC SC for review. The PJCIS requested Dr Renwick 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 was also required to review the Assistance and Access Act pursuant to subsection 6(1D) of the *Independent National Security Legislation Monitor Act 2010*.

On 30 June 2020, Dr Renwick provided his completed review of the Assistance and Access Act to the Attorney-General and the PJCIS in fulfilment of both the INSLM's legislative requirement and the referral by the PJCIS. The Attorney-General tabled the report in Parliament on 9 July 2020.

Dr Renwick made 33 recommendations to reform the powers granted and modified by the Assistance and Access Act. The Government will consider the recommendations of Dr Renwick's report, alongside any recommendations made by the PJCIS, once it issues its report on its third review of the Assistance and Access Act.

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

The PJCIS was due to conclude its third review of the Assistance and Access Act by 30 September 2020. This review will build on the findings of the review of the then INSLM and two previous PJCIS reviews. At the time this report was provided to the Minister for Home Affairs, the PJCIS had not yet handed down its report on the third review.

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

- PJCIS Data Retention review: <www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Dataretentionregime>
- INSLM Assistance and Access review: <www.inslm.gov.au/reviews-reports/telecommunications-and-other-legislation-amendment-act-2018-related-matters>
- PJCIS first review of Assistance and Access: <www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/TelcoAmendmentBill2018/Report_1>
- PJCIS second review of Assistance and Access: <www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/ReviewofTOLAAct/Report>
- PJCIS third review of Assistance and Access: <www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/AmendmentsTOLAAct2018>

Key findings

The following key statistics are relevant to the 2019–20 reporting period.

- 3,677 interception warrants were issued to interception agencies. This was an increase of 116 on the 3,561 issued in 2018–19.
- The majority of serious offences that were specified in interception warrants issued were serious drug and trafficking offences (2,096 times specified), followed by loss of life or personal injury offences (616 times specified) and murder (303 times specified).
- Information obtained under interception warrants was used in:[1]
    - 2,685 arrests;
    - 5,219 prosecutions; and
    - 2,652 convictions.
- 1,385 stored communications warrants were issued to criminal law-enforcement agencies, an increase of 132 on the 1,253 issued in 2018–19.
- Law enforcement agencies made 542 arrests, conducted 568 proceedings, and obtained 298 convictions involving evidence obtained under stored communications warrants.
- 20 enforcement agencies made 311,312 authorisations for the disclosure of historical telecommunications data – an increase of 15,621 authorisations from the 295,691 authorisations made in 2018–19. Of these, 306,995 were made to enforce the criminal law.
- The majority of criminal law offences for which historical telecommunications data was requested were illicit drug offences (78,142 requests), followed by 32,827 requests for fraud and related offences and 24,834 requests for robbery offences.
- 32,856 authorisations were made by criminal law-enforcement agencies for the disclosure of prospective telecommunications data, an increase of 5,085 on the 27,771[2] authorisations made in 2018–19.
- One journalist information warrant was issued to the QLD CCC, under which one historical data authorisation was made for the enforcement of the criminal law.
- Three agencies used powers under Part 15 of the *Telecommunications Act 1997* (Telecommunications Act) to request technical assistance from designated communications providers. One technical assistance request was given by the ACIC, while three were given by the AFP, and seven were given by NSW Police.

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

[2] NT Police identified corrections regarding historic telecommunications data for the 2017–18 and 2018–19 reporting periods. The amended total number of authorisations for 2018–19 period is 27,771, inclusive of corrected NT Police figures. Appendix D provides both the original figures reported for the 2017–18 and 2018–19 periods, and the amended figures as identified and corrected.

Access to the content of a communication

Accessing content, or the substance of a communication — for instance, the message written in an email, the discussion between two parties to a phone call, the subject line of an email or a private social media post — without the knowledge of the person making the communication is highly intrusive. Under the TIA Act, unless access occurs in certain limited circumstances, such as a life threatening emergency, interception or access to stored communications can only occur under either an interception or stored communications warrant. Access to a person's communications is subject to significant safeguards, oversight and reporting obligations. This 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.[3]

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.

During the 2019–20 reporting period all enforcement agencies could access historical data[4] and only criminal law-enforcement agencies[5] could access prospective data to assist in the investigation of offences punishable by at least three years' imprisonment.[6]

The Data Retention Act reduced the number of enforcement agencies that could access telecommunications data under the TIA Act to 20 specified agencies. The Minister for Home Affairs may declare additional agencies in limited circumstances for a period of 40 sitting days of Parliament. No additional agencies were declared in the 2019–20 reporting period.

Section 280 of the Telecommunications Act provides an exemption to the general prohibition on the disclosure of telecommunications in sections 276, 277 and 278 of that

[3] 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.
[4] 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.
[5] All 'criminal law-enforcement agencies' are set out in section 110A of the TIA Act. These agencies include all interception agencies as well as Home Affairs, ASIC, and the ACCC.
[6] Prospective data is telecommunications data that comes into existence during a period of time in which an authorisation is in force.

Act, allowing agencies outside of the data retention scheme to use their own powers to seek access if the disclosure is required or authorised under law. Requests under section 280(1)(b) are facilitated by industry obligations under section 313(3) of the Telecommunications Act, which requires carriers and carriage service providers to give authorities such help as is reasonable necessary. This is a licencing condition for all carriers.

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; and
- Chapter 4 – industry technical assistance.

The TIA Act, Telecommunications Act and associated legislation 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 Infrastructure, Transport, Regional Development and Communications <www.communications.gov.au>
- Commonwealth Ombudsman <www.ombudsman.gov.au>
- Office of the Australian Information Commissioner <www.oaic.gov.au>
- Telecommunications Industry Ombudsman <www.tio.com.au>
- Australian Communications and Media Authority <www.acma.gov.au>

CHAPTER 1 – TELECOMMUNICATIONS INTERCEPTION

The interception of communications is regulated by Chapter 2 of the TIA Act. The primary function of Chapter 2 is to prohibit 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. This protects the privacy of the communications of people who use the Australian telecommunications network.

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, State and Territory police forces and integrity agencies. 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 live phone call between two parties). 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 abuse, money laundering, and offences involving organised crime.

Paragraphs 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 2019–20 the majority of warrants obtained were to assist with investigations into serious drug offences (2,096 warrants). Loss of life or personal injury offences were specified in 616 warrants and 303 related to murder investigations. Money laundering was specified as an offence in 272 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 C.

[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 – paragraphs 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
Administration of justice / government offences	-	5	17	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**22**
Assisting person to escape or dispose of proceeds	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	-	**1**
Bribery, corruption and dishonesty offences	-	-	13	41	23	7	17	11	-	-	29	9	6	2	-	-	5	**163**
Cartel offences	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**0**
Child abuse offences	-	-	14	-	-	-	-	-	-	-	1	-	-	-	-	1	-	**16**
Conspire/aid/abet serious offence	16	-	-	-	-	-	6	-	-	-	16	-	-	2	-	5	-	**45**
Cybercrime offences	-	-	8	-	-	-	-	-	-	-	4	-	-	-	-	-	-	**12**
Espionage and foreign interference	-	-	3	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**3**
Kidnapping	-	-	1	-	-	-	-	-	-	-	66	-	-	1	-	-	1	**69**
Loss of life or personal injury	-	-	23	-	-	-	-	-	-	-	455	-	33	4	3	40	58	**616**
Money laundering	85	-	117	-	-	-	-	-	-	28	9	21	-	3	-	-	9	**272**
Murder	-	-	19	-	-	-	-	-	-	3	209	-	14	3	4	27	24	**303**

Offences involving planning and organisation	1	-	13	-	-	-	-	-	-	-	134	-	-	-	-	7	18	**173**
Organised offences and/or criminal organisations	5	-	10	-	-	-	-	-	-	1	17	-	-	-	-	-	-	**33**
People smuggling and related	-	-	9	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**9**
Serious damage to property and/or serious arson	-	-	4	-	-	-	-	-	1	-	40	-	-	2	-	6	11	**64**
Serious drug offences and/or trafficking	197	-	464	-	-	-	-	3	17	121	816	4	202	20	6	50	196	**2,096**
Serious fraud	3	-	23	1	1	-	-	-	-	4	57	13	1	1	-	3	1	**108**
Serious loss of revenue	20	-	29	-	-	-	-	-	-	-	2	-	-	2	-	3	-	**56**
Special ACC investigations	44	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**44**
Telecommunications offences	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**0**
Terrorism financing offences	5	-	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**7**
Terrorism offences	-	-	113	-	-	-	-	-	-	-	4	-	-	-	-	1	-	**118**
TOTAL	**376**	**5**	**882**	**42**	**24**	**7**	**23**	**14**	**18**	**157**	**1,860**	**47**	**256**	**40**	**13**	**143**	**323**	**4,230**

Eligibility to issue a telecommunications 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; and
- Federal Circuit Court.

Persons who hold one of the following appointments to the AAT may be nominated by the Attorney-General to issue warrants under Part 2-5 of the TIA Act:

- Deputy President;
- senior member (of any level); and
- member (of any level).

Paragraph 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 2019–20 there were 93 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 – paragraph 103(ab)

Issuing Authority	Number eligible
Federal Court judges	13
Family Court judges	10
Federal Circuit Court judges	34
Nominated AAT members	36
TOTAL	**93**

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 2019–20.

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

Agency	Issuing Authority				
	Family Court judges	Federal Circuit Court judges	Federal Court judges	Nominated AAT members	TOTAL
ACIC	10	6	92	1	**109**
ACLEI	-	-	-	3	**3**
AFP	-	48	-	588	**636**
CCC (WA)	41	-	-	-	**41**
IBAC	-	-	-	24	**24**
ICAC (NSW)	-	-	-	7	**7**
ICAC (SA)	-	5	-	18	**23**
LECC	-	-	-	14	**14**
NT Police	-	18	-	-	**18**
NSW CC	-	-	-	144	**144**
NSW Police	-	-	53	1,807	**1,860**
QLD CCC	-	2	-	25	**27**
QLD Police	-	201	-	55	**256**
SA Police	-	-	1	35	**36**
TAS Police	-	-	-	13	**13**
VIC Police	-	-	-	143	**143**
WA Police	255	-	-	68	**323**
TOTAL	**306**	**280**	**146**	**2,945**	**3,677**

Applications for telecommunications interception warrants

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

Table 4 presents this information. In 2019–20 agencies were issued 3,677 interception warrants, an increase of 116 from 2018–19, where 3,561 warrants were issued. 737 renewals of interception warrants were issued in 2019–20.

Table 4: Applications, telephone applications and renewal applications for telecommunications interception warrants[8] – paragraphs 100(1)(a)-(c) and 100(2)(a)-(c)

Agency	Relevant Statistics	Applications for warrants		Telephone applications for warrants		Renewal applications	
		18/19	19/20	18/19	19/20	18/19	19/20
ACIC	Made	133	109	-	2	14	23
	Refused	1	-	-	-	-	-
	Issued	132	109	-	2	14	23
ACLEI	Made	11	3	-	-	6	-
	Refused	-	-	-	-	-	-
	Issued	11	3	-	-	6	-
AFP	Made	634	638	-	-	201	229
	Refused	-	2	-	-	-	-
	Issued	634	636	-	-	201	229
CCC (WA)	Made	14	41	-	-	-	11
	Refused	-	-	-	-	-	-
	Issued	14	41	-	-	-	11
IBAC	Made	20	26	-	-	3	2
	Refused	3	2	-	-	-	-
	Issued	17	24	-	-	3	2
ICAC (NSW)	Made	19	7	-	-	5	-
	Refused	-	-	-	-	-	-
	Issued	19	7	-	-	5	-
ICAC (SA)	Made	19	23	-	-	4	11
	Refused	-	-	-	-	-	-
	Issued	19	23	-	-	4	11
LECC	Made	18	14	-	-	-	6
	Refused	-	-	-	-	-	-

[8] The telephone applications and renewal applications made, refused and issued for interception warrants are a subset of the total warrants made, refused, and issued for each agency.

	Issued	18	14	-	-	-	6
NT Police	Made	18	18	-	-	-	-
	Refused	1	-	-	-	-	-
	Issued	17	18	-	-	-	-
NSW CC	Made	131	144	-	-	25	34
	Refused	-	-	-	-	-	-
	Issued	131	144	-	-	25	34
NSW Police	Made	1,613	1,860	41	39	384	330
	Refused	-	-	-	-	-	-
	Issued	1,613	1,860	41	39	384	330
QLD CCC	Made	28	27	-	-	7	6
	Refused	-	-	-	-	-	-
	Issued	28	27	-	-	7	6
QLD Police	Made	297	256	-	-	52	44
	Refused	-	-	-	-	-	-
	Issued	297	256	-	-	52	44
SA Police	Made	62	36	-	1	3	3
	Refused	-	-	-	-	-	-
	Issued	62	36	-	1	3	3
TAS Police	Made	22	13	-	-	-	1
	Refused	-	-	-	-	-	-
	Issued	22	13	-	-	-	1
VIC Police	Made	170	146	5	-	10	17
	Refused	-	3	-	-	-	-
	Issued	170	143	5	-	10	17
WA Police	Made	364	323	-	-	33	20
	Refused	7	-	-	-	-	-
	Issued	357	323	-	-	33	20
TOTAL	**Made**	**3,573**	**3,684**	**46**	**42**	**747**	**737**
	Refused	**12**	**7**	**0**	**0**	**0**	**0**
	Issued	**3,561**	**3,677**	**46**	**42**	**747**	**737**

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.

Paragraphs 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 2019–20, there were no interception warrants issued that authorised entry on to premises to carry out telecommunications interception. This is a decrease compared to the 2018–19 reporting period, in which three interception warrants authorising entry onto premises were issued to the AFP.

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

Agency	Relevant statistics	Warrants authorising entry on premises	
		18/19	19/20
AFP	Made	3	-
	Refused	-	-
	Issued	3	-
TOTAL	**Made**	**3**	**0**
	Refused	**0**	**0**
	Issued	**3**	**0**

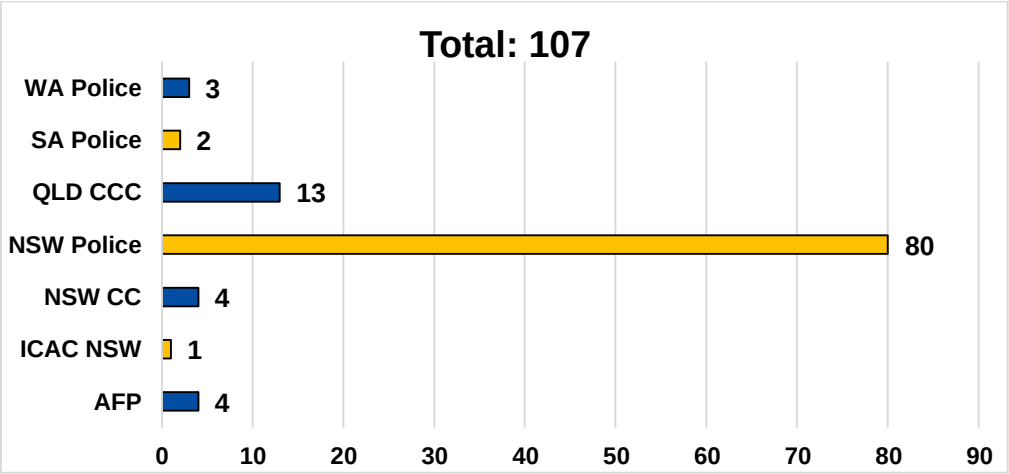
Conditions or restrictions on warrants

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.

Paragraphs 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 2019–20, 107 interception warrants were issued with a condition or restriction, an increase of 89 compared to the 18 issued in the 2018–19 reporting period.

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



Effectiveness of telecommunications interception warrants

Paragraphs 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 of the agency's functions, and on the basis of information that was, or included, lawfully intercepted information.

Agencies also 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.

Paragraphs 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 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 2019–20 there were 2,685 arrests made as a result of lawfully intercepted information. There were also 5,219 prosecutions and 2,652 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, one arrest 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 – paragraphs 102(1)(a) and 102(2)(a)

Agency	18/19		19/20	
	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	-	30	-	17
ACLEI	-	1	-	-
AFP	169	166	137	54
ICAC (SA)	2	-	-	5
NT Police	16	-	18	9
NSW CC	-	69	-	69
NSW Police	1,218	58	1,378	5
QLD CCC	24	1	8	-
QLD Police	423	-	390	-
SA Police	36	-	34	-
TAS Police	26	-	1	10
VIC Police	280	70	289	42
WA Police	394	-	430	364
TOTAL	**2,588**	**395**	**2,685**	**575**

Table 7: Prosecutions per offence category in which lawfully intercepted information was given in evidence – paragraphs 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
Administration of justice / government offences	-	-	3	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**3**
Assisting person to escape or dispose of proceeds	-	-	-	-	-	-	-	-	-	1	-	-	1	-	-	-	-	**2**
Bribery or corruption	-	-	-	-	9	-	1	-	-	2	5	-	-	-	-	-	37	**54**
Cartel offences	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**0**
Child abuse offences	-	-	-	-	-	-	-	-	-	-	2	-	-	-	-	-	11	**13**
Conspire/aid/abet serious offence	-	-	2	-	-	-	-	-	1	6	1	-	1	-	-	5	7	**23**
Cybercrime offences	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**0**
Espionage and foreign interference	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**0**
Kidnapping	-	-	-	-	-	-	-	-	-	1	13	-	1	-	-	-	-	**15**
Loss of life	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	6	4	**11**
Money laundering	1	-	41	-	-	-	-	-	-	104	49	1	-	-	-	12	38	**246**
Murder	-	-	-	-	-	-	-	-	-	6	18	-	-	-	1	4	8	**37**
Offences against the TIA Act	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**0**
Offences involving planning and organisation	1	-	-	-	-	-	-	-	-	-	201	-	-	-	-	11	490	**703**
Organised crime	-	-	17	-	-	-	-	-	-	29	7	-	-	-	-	-	-	**53**
Other offence punishable by 3 years to life	-	-	13	-	-	-	-	-	-	-	15	-	112	-	-	32	-	**172**
People smuggling and related	-	-	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**2**
Serious arson	-	-	-	-	-	-	-	-	1	1	7	-	-	-	-	3	2	**14**
Serious damage to property	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	18	**18**

Serious drug offence and/or trafficking	8	-	113	-	-	-	-	-	16	120	1,495	-	14	4	6	76	1,728	**3,580**
Serious fraud	-	-	8	-	-	-	-	1	-	131	16	-	2	-	-	5	-	**163**
Serious loss of revenue	-	-	-	-	-	-	-	-	-	6	-	-	-	-	-	-	-	**6**
Serious personal injury	-	-	-	-	-	-	-	-	-	1	61	-	4	-	1	23	8	**98**
Special ACC investigations	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**0**
Telecommunications offences	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**0**
Terrorism offences	-	-	6	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**6**
Terrorism financing offences	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**0**
Total	**10**	**0**	**205**	**0**	**9**	**0**	**1**	**1**	**18**	**409**	**1,890**	**1**	**135**	**4**	**8**	**177**	**2,351**	**5,219**

Table 8: Convictions per offence category in which lawfully intercepted information was given in evidence – paragraphs 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
Administration of justice / government offences	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**1**
Assisting person to escape or dispose of proceeds	-	-	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	**1**
Bribery or corruption	-	-	-	41	9	-	1	-	-	1	2	-	-	-	-	-	10	**64**
Cartel offences	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**0**
Child abuse offences	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	5	**5**
Conspire/aid/abet serious offence	-	-	2	-	-	-	-	-	-	3	-	-	1	-	-	5	3	**14**
Cybercrime offences	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**0**
Espionage and foreign interference	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**0**

Kidnapping	-	-	-	-	-	-	-	-	-	1	7	-	1	-	-	-	-	**9**
Loss of life	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	4	1	**6**
Money laundering	1	-	19	-	-	-	-	-	-	38	-	1	-	-	-	12	16	**87**
Murder	-	-	3	-	-	-	-	-	-	2	8	-	-	2	-	4	2	**21**
Offences against the TIA Act	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**0**
Offences involving planning and organisation	1	-	-	-	-	-	-	-	-	-	33	-	-	-	-	11	286	**331**
Organised crime	-	-	15	-	-	-	-	-	-	7	6	-	-	-	-	-	-	**28**
Other offence punishable by three years to life	-	-	11	-	-	-	-	-	-	-	16	-	111	-	-	29	-	**167**
People smuggling and related	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**0**
Serious arson	-	-	-	-	-	-	-	-	1	1	-	-	-	-	-	-	-	**2**
Serious damage to property	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	8	**9**
Serious drug offence and/or trafficking	8	-	55	-	-	-	-	-	15	58	363	-	14	4	-	70	1,260	**1,847**
Serious fraud	-	-	3	1	-	-	-	-	-	1	16	-	-	-	-	-	-	**21**
Serious loss of revenue	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	-	-	**1**
Serious personal injury	-	-	-	-	-	-	-	-	-	-	11	-	4	-	-	19	2	**36**
Special ACC investigations	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Telecommunications offences	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**0**
Terrorism offences	-	-	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**2**
Total	**10**	**0**	**111**	**42**	**9**	**0**	**1**	**0**	**16**	**114**	**463**	**1**	**132**	**6**	**0**	**154**	**1,593**	**2,652**

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) that relate to a particular person. 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.

Paragraphs 100(1)(ea) and 100(2)(ea) provide that this report must set out the relevant statistics about written applications, oral 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 2019–20, 641 named person warrants were issued, an increase of 5 from the 2018–19 reporting period in which 636 named person warrants were issued.

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

Agency	Relevant Statistics	Applications for named person warrants		Telephone applications for named person warrants		Renewal applications for named person warrants	
		18/19	19/20	18/19	19/20	18/19	19/20
ACIC	Made	55	54	-	2	10	17
	Refused	-	-	-	-	-	-
	Issued	55	54	-	2	10	17
AFP	Made	186	224	-	-	53	97
	Refused	-	-	-	-	-	-
	Issued	186	224	-	-	53	97
CCC (WA)	Made	1	3	-	-	-	1
	Refused	-	-	-	-	-	-
	Issued	1	3	-	-	-	1
IBAC	Made	2	1	-	-	-	-

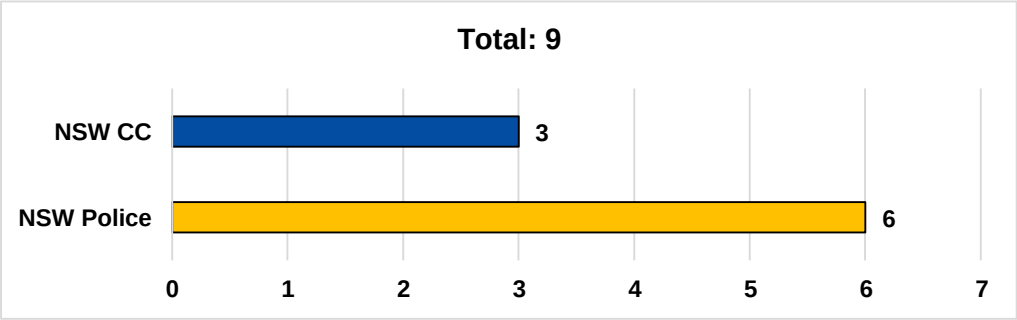
[9] The telephone applications and renewal applications made, refused and issued for named person warrants are a subset of the total warrants made, refused, and issued for each agency.

Agency	Relevant Statistics	Applications for named person warrants		Telephone applications for named person warrants		Renewal applications for named person warrants	
		18/19	19/20	18/19	19/20	18/19	19/20
	Refused	-	-	-	-	-	-
	Issued	2	1	-	-	-	-
LECC	Made	-	4	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	-	4	-	-	-	-
NT Police	Made	1	-	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	1	-	-	-	-	-
NSW CC	Made	66	52	-	-	19	16
	Refused	-	-	-	-	-	-
	Issued	66	52	-	-	19	16
NSW Police	Made	83	121	-	-	26	31
	Refused	-	-	-	-	-	-
	Issued	83	121	-	-	26	31
QLD CCC	Made	3	-	-	-	1	-
	Refused	-	-	-	-	-	-
	Issued	3	-	-	-	1	-
QLD Police	Made	55	43	-	-	11	4
	Refused	-	-	-	-	-	-
	Issued	55	43	-	-	11	4
SA Police	Made	4	2	-	-	1	-
	Refused	-	-	-	-	-	-
	Issued	4	2	-	-	1	-
TAS Police	Made	5	1	-	-	-	1
	Refused	-	-	-	-	-	-
	Issued	5	1	-	-	-	1
VIC Police	Made	53	57	1	-	4	11
	Refused	-	1	-	-	-	-
	Issued	53	56	1	-	4	11
WA Police	Made	122	80	-	-	13	6
	Refused	-	-	-	-	-	-
	Issued	122	80	-	-	13	6

Agency	Relevant Statistics	Applications for named person warrants		Telephone applications for named person warrants		Renewal applications for named person warrants	
		18/19	19/20	18/19	19/20	18/19	19/20
Total	Made	636	642	1	2	138	184
	Refused / Withdrawn	0	1	0	0	0	0
	Issued	636	641	1	2	138	184

In 2019–20, nine named person warrants were issued with a condition or restriction. This is an increase of one compared to the eight issued with a condition or restriction in the 2018–19 period.

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



Paragraphs 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 2019–20 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 – paragraphs 100(1)(eb) and 100(2)(eb)

Agency	Number of services							
	1 service only		2 – 5 services		6 – 10 services		10+ services	
	18/19	19/20	18/19	19/20	18/19	19/20	18/19	19/20
ACIC	20	23	28	25	7	5	1	-
AFP	55	92	113	116	13	8	1	5
CCC (WA)	-	1	-	1	-	-	1	1
IBAC	-	-	2	1	-	-	-	-
LECC	-	-	-	3	-	1	-	-
NT Police	-	-	1	-	-	-	-	-
NSW CC	37	26	29	25	-	1	-	-
NSW Police	14	48	43	69	-	4	2	-

Agency	Number of services							
	1 service only		2 – 5 services		6 – 10 services		10+ services	
	18/19	19/20	18/19	19/20	18/19	19/20	18/19	19/20
QLD CCC	1	-	2	-	-	-	-	-
QLD Police	14	10	37	28	4	4	-	1
SA Police	3	1	1	1	-	-	-	-
TAS Police	2	-	2	1	1	-	-	-
VIC Police	9	20	35	23	3	2	-	-
WA Police	39	26	81	52	2	-	-	-
TOTAL	**194**	**247**	**374**	**345**	**30**	**25**	**5**	**7**

Under the TIA Act, agencies can apply for a named person warrant in relation to telecommunications devices, where a device or devices of interest can be identified.

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

i. services intercepted under service-based named person warrants;

ii. services intercepted under device based named person warrants; and

iii. telecommunications devices intercepted under device-based named person warrants.

Figure 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 – paragraphs 100(1)(ec) and 100(2)(ec)

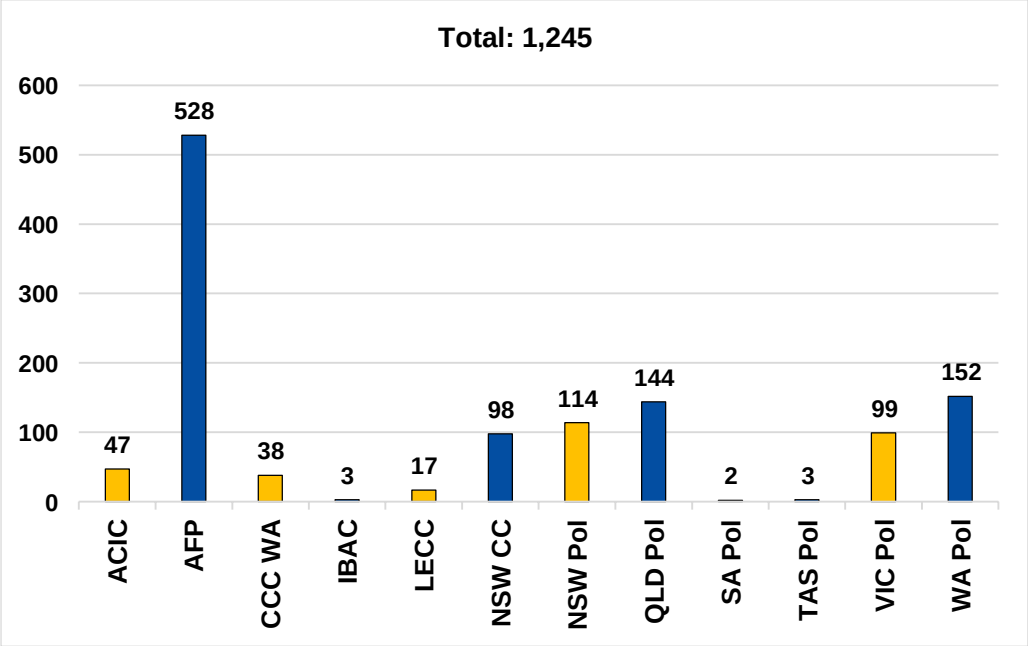


Table 11 shows that in 2019–20, device based named person warrants were used by only a small number of agencies. This is consistent with the 2018–19 reporting period.

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

Agency	Devices		Services	
	18/19	19/20	18/19	19/20
ACIC	4	21	4	17
AFP	48	61	291	304
NSW CC	7	-	-	3
NSW Police	15	15	18	19
VIC Police	6	11	-	-
WA Police	-	2	-	-
TOTAL	**80**	**110**	**313**	**343**

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.

Paragraphs 100(1)(ed) and 100(2)(ed) provide that this report must set out the relevant statistics about written applications, oral 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 2019–20, 98 B-Party warrants were issued to interception agencies. This represents a decrease of 20 from the 118 B-Party warrants issued in 2018–19.

Table 12: Applications for B-Party warrants, telephone applications for B-Party warrants, and renewal applications – paragraphs 100(1)(ed) and 100(2)(ed)[10]

Agency	Relevant Statistics	Applications for B-Party Warrants		Telephone applications for B-Party warrants		Renewal applications for B-Party warrants	
		18/19	19/20	18/19	19/20	18/19	19/20
ACIC	Made	-	2	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	-	2	-	-	-	-
AFP	Made	66	31	-	-	50	17
	Refused	-	-	-	-	-	-
	Issued	66	31	-	-	50	17
NSW CC	Made	3	3	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	3	3	-	-	-	-
NSW Police	Made	46	60	5	13	2	3
	Refused	-	-	-	-	-	-
	Issued	46	60	5	13	2	3
SA Police	Made	1	1	-	1	-	-
	Refused	-	-	-	-	-	-
	Issued	1	1	-	1	-	-
VIC Police	Made	2	-	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	2	-	-	-	-	-
WA Police	Made	-	1	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	-	1	-	-	-	-
TOTAL	**Made**	**118**	**98**	**5**	**14**	**52**	**20**
	Refused	**0**	**0**	**0**	**0**	**0**	**0**
	Issued	**118**	**98**	**5**	**14**	**52**	**20**

In 2019–20, seven B-Party warrants were issued with conditions or restrictions for authorised entry on premises. This is an increase from zero in the 2018–19 reporting period.

[10] The telephone applications and renewal applications made, refused and issued for B-Party warrants are a subset of the total warrants made, refused, and issued for each agency.

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

Agency	B-party warrants specifying conditions or restrictions	
	18/19	19/20
NSW Police	-	6
WA Police	-	1
TOTAL	0	7

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.

Paragraphs 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 – paragraphs 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	87	63	87	87
ACLEI	90	-	-	-
AFP	83	87	86	81
CCC (WA)	90	74	90	73
IBAC	84	80	-	-
ICAC (NSW)	90	58	-	-
ICAC (SA)	62	41	70	62
LECC	90	69	90	85
NT Police	90	62	-	-
NSW CC	82	60	85	67
NSW Police	45	34	65	55
QLD CCC	80	79	81	81
QLD Police	80	59	76	62
SA Police	62	37	77	90
TAS Police	80	74	90	41
VIC Police	83	52	75	65

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)
WA Police	86	52	90	59
AVERAGE	**80**	**58**	**82**	**70**

A single B-Party warrant can be in force for up to 45 days. Paragraphs 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 – paragraphs 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)
ACIC	45	45	-	-
AFP	45	41	45	42
NSW CC	43	8	-	-
NSW Police	31	17	34	34
SA Police	15	5	-	-
WA Police	45	5	-	-
AVERAGE	**37**	**20**	**40**	**38**

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. Paragraphs 101(1)(e) and 101(2)(e) of the TIA Act provide that this report must set out how many final renewals ceased to be in force during that year. 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 – paragraphs 101(1)(e) and 101(2)(e)

Agency	90 days		150 days		180 days	
	18/19	19/20	18/19	19/20	18/19	19/20
ACIC	3	6	4	3	2	3
ACLEI	1	-	1	-	2	-
AFP	5	4	29	12	41	39
CCC (WA)	-	-	-	11	-	-
IBAC	-	-	6	-	-	-
ICAC (NSW)	-	-	-	-	3	-
LECC	4	1	1	1	-	4
NSW CC	2	7	9	1	8	1
NSW Police	129	118	20	28	43	50
QLD CCC	2	-	5	2	-	2
QLD Police	19	15	17	17	6	7
SA Police	-	-	3	1	-	-
TAS Police	-	1	-	-	-	-
VIC Police	5	5	-	4	-	-
WA Police	12	6	27	3	3	3
TOTAL	**182**	**163**	**122**	**83**	**108**	**109**

Eligible warrants

Subsections 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.

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.

Table 17 presents this information. In 2019–20, 73 per cent of total warrants were eligible warrants.

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

Agency	Total number of warrants	Number of eligible warrants	%
ACIC	133	72	54
ACLEI	3	-	0
AFP	740	445	60
CCC (WA)	52	7	13
IBAC	25	12	48
ICAC (NSW)	7	5	71
ICAC (SA)	29	13	45
LECC	18	3	17
NT Police	21	18	86
NSW CC	166	114	69
NSW Police	2,085	1,765	85
QLD CCC	27	18	67
QLD Police	291	282	97
SA Police	56	44	79
TAS Police	14	6	43
VIC Police	167	107	64
WA Police	395	187	47
TOTAL / AVERAGE	**4,229**	**3,098**	**73**

Interception without a warrant

Under subsections 7(4) and (5) of the TIA Act, the AFP 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 where an officer or staff member of the agency intercepted a communication in reliance on subsections 7(4) or (5).

In 2019–20, there were no instances where agencies intercepted communications under subsections 7(4) or (5) of the TIA Act without a warrant.

International assistance

Section 102B of the TIA Act provides that this report must set out the number of occasions where 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 2019–20, there were two occasions in which lawfully intercepted information was provided to a foreign country under subsection 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. Paragraph 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 18: Number of interceptions carried out on behalf of other agencies – paragraph 103(ac)

Interception carried out by:	Interception carried out on behalf of:	Number of interceptions
ACIC	QLD CCC	27
AFP	ACLEI	3
CCC WA	ICAC (SA)	23
NSW CC	NSW POL	2
VIC Police	TAS Police	13
TOTAL		**68**

Telecommunications interception expenditure

Table 19 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 19: Total expenditure incurred by each agency in connection with the execution of telecommunications interception warrants and average expenditure per telecommunications interception warrant – paragraphs 103(a) and 103(aa)

Agency	Total expenditure	Average expenditure
ACIC	$6,526,696	$59,878
ACLEI	$11,898	$3,966
AFP	$12,406,298	$19,507
CCC (WA)	$646,657	$15,772
IBAC	$825,484	$34,395
ICAC (NSW)	$736,489	$105,213
ICAC (SA)	$227,450	$9,889
LECC	$610,264	$43,590
NT Police	$792,851	$44,047
NSW CC	$2,165,242	$15,036
NSW Police	$9,293,791	$4,997
QLD CCC	$1,769,877	$65,551
QLD Police	$5,636,217	$22,016
SA Police	$3,758,396	$104,400
TAS Police	$892,383	$68,645
VIC Police	$669,558	$4,682
WA Police	$3,876,160	$12,000
TOTAL / AVERAGE	**$50,845,711**	**$37,270**

Table 20 and Figure 4 provide 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 20: Recurrent interception costs per agency

Agency	Salaries	Administrative Support	Capital expenditure	Interception costs	Total ($)
ACIC	$4,150,007	$193,848	$680,341	$1,502,498	**$6,526,694**
ACLEI	$336,721	$81,075	-	$1,716	**$419,512**
AFP	$8,793,431	$177,705	-	$3,435,162	**$12,406,298**
CCC (WA)	$271,075	$1,004	$312,442	$62,136	**$646,657**
IBAC	$636,839	$7,799	$80,299	$100,547	**$825,484**
ICAC (NSW)	$240,386	-	-	$496,103	**$736,489**
ICAC (SA)	$142,560	-	-	$84,890	**$227,450**
LECC	$497,152	$52,500	$12,363	$48,429	**$610,444**
NT Police	$389,134	$156,258	$179,854	$67,605	**$792,851**
NSW CC	$1,513,745	$76,131	-	$575,366	**$2,165,242**
NSW Police	$6,884,963	$369,613	-	$2,039,215	**$9,293,791**
QLD CCC	$1,142,057	$249,179	$14,729	$363,913	**$1,769,878**
QLD Police	$4,601,157	$672,542	-	$362,517	**$5,636,216**
SA Police	$2,317,649	$98,448	$303,758	$1,038,541	**$3,758,396**
TAS Police	$705,979	$11,146	$558	$174,700	**$892,383**
VIC Police	$424,111	$7,284	$156,000	$53,563	**$640,958**
WA Police	$3,396,866	$268,225	-	$211,069	**$3,876,160**
TOTAL	**$36,443,832**	**$2,422,757**	**$1,740,344**	**$10,617,970**	**$51,224,903**

Emergency service facilities

Under the TIA Act, listening to or recording calls to and from a facility declared by the Minister for Home Affairs 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 21 sets out the number of places that have been declared under the TIA Act to be emergency service facilities.

Table 21: Emergency service facility declarations – paragraph 103(ad)

Agency	Police	Fire brigade	Ambulance	Emergency services authority	Despatching
Australian Capital Territory	5	-	-	-	4
New South Wales	8	94	6	-	6
Northern Territory	2	-	1	1	4
Queensland	21	12	9	-	14
South Australia	1	2	1	-	4
Tasmania	1	2	1	-	2
Victoria	-	-	3	-	10
Western Australia	1	2	1	-	6
TOTAL	**39**	**112**	**22**	**1**	**50**

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 Home Affairs with a copy of each telecommunications interception warrant;
- interception agencies to report to the Minister for Home Affairs, 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 Home Affairs 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 for Home Affairs to inspect.

Law enforcement agencies' use of interception powers under the TIA Act is independently overseen by the Commonwealth Ombudsman and equivalent state oversight and integrity 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 2019.

The Commonwealth Ombudsman is required under the TIA Act to report to the Minister for Home Affairs 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 for Home Affairs. The Commonwealth Ombudsman also conducts inspections of records in relation to access by enforcement agencies (including both Commonwealth and state agencies) to stored communications and telecommunications data. The Data Retention Act introduced additional obligations for these reports to be provided to the Minister for Home Affairs and tabled in Parliament.

Commonwealth Ombudsman – inspection of telecommunications interception records

During the reporting period the Commonwealth Ombudsman conducted five inspections of the interception records of the ACIC, ACLEI, and the AFP (two inspections for ACIC and AFP; one inspection for ACLEI) – refer to Table 22.

During its review of warrants that expired or were revoked in the period between 1 January and 31 December 2019, 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 appropriate disclosure of compliance issues.

The Ombudsman's inspection criteria 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 subsection 39(1) and section 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?
- Are agencies cooperative and frank with the inspections performed by the Commonwealth Ombudsman?

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 complement TIA Act powers, this ensures the Commonwealth Ombudsman can oversight their collective use.

Commonwealth Ombudsman's summary of findings

Table 22: Summary of findings from the inspections conducted at each Commonwealth agency in 2019–20 – paragraph 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)?	Two instances of non-compliance.	Compliant.	Three instances of non-compliance.
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, with minor exceptions.	Compliant.	Compliant.
Were interceptions conducted in accordance with the warrants (s 7) and was any unlawfully intercepted information properly dealt with (s 63)?	Three instances where compliance could not be determined, two instances of non-compliance.	Compliant.	Seven instances where compliance could not be determined, one instance of non-compliance.
Are agencies cooperative and frank with the inspections performed by the Commonwealth Ombudsman?	Compliant.	Compliant.	Compliant.

Commonwealth Ombudsman's findings per Commonwealth agency for warrants expiring between 1 January to 31 December 2019

Section 79: Destruction of restricted records

Section 79 of the TIA Act sets out the requirements for agencies when destroying restricted records.

Subsection 79(1) of the TIA Act provides that, where the chief officer of the agency is satisfied that a restricted record is not likely to be required for a permitted purpose, the chief officer shall cause the restricted record to be destroyed forthwith. Subsection 79(2) states that a restricted record must not be destroyed unless the agency has received from the Secretary of the Department, (being the Department of Home Affairs) written notice that the entry in the General Register relating to the warrant under which the record was obtained has been inspected by the Minister for Home Affairs.

At the Ombudsman's first inspection of the AFP, the Ombudsman identified one instance where it could not locate the notice from the Secretary of the Department. In turn, it appeared the AFP may have destroyed the restricted record contrary to the requirements of subsection 79(2) of the TIA Act.

At the Ombudsman's second inspection of the AFP, three separate issues relating to the destruction of records were identified:

1. The AFP destroyed restricted records in accordance with section 79 before the Ombudsman had an opportunity to inspect the relevant files. While there is no legislative requirement to preserve information for the purposes of the Ombudsman's inspections, all agencies have an obligation under Part 2.7 of the TIA Act to retain records to facilitate the Ombudsman's oversight functions. As there was no product to inspect, the Ombudsman could not assess whether the interception accorded with the warrant. As a result the Ombudsman suggested the AFP retain all records and intercepted information in relation to warrants until such time as the Ombudsman assesses the AFP's compliance. In response to this finding the AFP implemented a quality assurance check to confirm, before they are destroyed, that warrants and associated data have been inspected by the Ombudsman.
2. The Ombudsman identified two warrants that were not destroyed 'forthwith' in line with the AFP's internal timeframes because staff had not included them in a destruction minute to a delegate of the chief officer for approval. The destruction of these warrants was postponed until another minute seeking approval to destroy warrants and associated data was prepared, resulting in a delay of approximately six weeks. In response to this finding and to avoid further breaches, the AFP increased its internal timeframes for the destruction process, from 14 business days to two months. The Ombudsman advised the AFP that they do not consider a period of two months meets the 'forthwith' requirements under subsection 150(1) and section 79 of the TIA Act. The Ombudsman asked the AFP to clarify why it extended the internal timeframe so significantly.

3. The Ombudsman identified one instance where a restricted record was destroyed and there was no evidence the Minister had inspected the relevant record on the General Register, contrary to the requirement set out in subsection 79(2) of the TIA Act. The AFP responded to this issue by notifying the Department that the record required inspection by the Minister. The AFP altered its process to have another member check the General Register before actioning destructions.

The Ombudsman did not assess ACLEI or the ACIC for compliance with section 79 of the TIA Act as both agencies advised they had not destroyed any restricted records during the relevant periods.

Section 80: Record keeping in connection with telecommunications interception warrants

Section 80 of the TIA Act requires the chief officer to cause to be kept certain documents connected with the issuing of telecommunications interception warrants. The Ombudsman considers agency compliance with record keeping requirements to be fundamental to demonstrating agency accountability for their use of covert and intrusive powers under the TIA Act.

The Ombudsman was satisfied that ACLEI was compliant with section 80 of the TIA Act, while the ACIC and AFP were compliant except for the instances described below.

In the Ombudsman's view all three agencies have sufficient record keeping procedures to achieve compliance with the TIA Act.

Australian Criminal Intelligence Commission

At the Ombudsman's first inspection the ACIC disclosed one instance where it had destroyed an original revocation instrument due to an administrative error. This is contrary to paragraph 80(c) of the TIA Act, which requires the agency to keep each instrument that revoked a warrant. The Ombudsman notes the ACIC printed a copy of the instrument from its systems and had it certified as true and correct by the officer who authorised the revocation.

The Ombudsman also identified one instance where there was no evidence that the ACIC had sent a notification under subsection 59A(2) to the Secretary of the Department of Home Affairs. Subsection 59A(2) of the TIA Act requires an agency to provide to the Secretary of the Department a written description of each service intercepted under a Named Person Warrant, if the service was not specified on the warrant.

Each written description under subsection 59A(2) must be kept by the agency in accordance with paragraph 80(b) of the TIA Act.

Following the inspection the ACIC located the notification and updated its records accordingly.

Australian Federal Police

At the Ombudsman's first inspection it was identified that the AFP had not kept two original warrants, contrary to paragraph 80(a) of the TIA Act, which requires the chief

officer to keep in their records each warrant issued to the agency. The AFP located one original warrant following the Ombudsman's inspection, but could not locate the other. The Ombudsman suggested the AFP take steps to ensure all original warrants are kept in accordance with the requirement in section 80 of the TIA Act. To raise awareness of this requirement of the TIA Act, the AFP communicated the Ombudsman's finding and suggestions about this issue to relevant AFP staff.

Despite this, during the second inspection the Ombudsman identified another instance where the AFP had not kept an original warrant. The Ombudsman suggested the AFP continue to take steps to ensure all original warrants are kept in accordance with the requirement of section 80 of the TIA Act, including providing training and raising awareness to investigators about the agency's obligations.

The Ombudsman was satisfied these instances of non-compliance were the result of administrative oversight and do not represent a systemic issue. However, the Ombudsman will continue to monitor this area of compliance at future inspections.

Section 81: Record keeping in connection with telecommunications interceptions

Section 81 of the TIA Act requires the chief officer to keep certain information in connection with interceptions, as well as to record particulars relating to restricted records and lawfully intercepted information.

The Ombudsman assessed that the AFP and ACLEI were compliant with section 81 of the TIA Act. The ACIC was assessed as compliant except for the instances described below. Despite these instances, the Ombudsman were satisfied that all agencies have sufficient record keeping procedures to achieve compliance with the TIA Act.

Australian Criminal Intelligence Commission

Paragraph 81(1)(e) of the TIA Act requires particulars of each use by the agency of lawfully intercepted information to be recorded as soon as possible after the use occurred. Paragraph 81(1)(f) requires particulars of each communication of lawfully intercepted information by an officer of the agency to a person or body that is not an officer of the agency to be recorded as soon as possible following the communication. The ACIC records instances of the use (internal) and communication (external) of legally intercepted information in a log.

The Ombudsman's second inspection identified that the log entries often contained generic language for the use and communication of legally intercepted information, such as 'weekly' and 'as required', rather than recording the particulars of each use. The ACIC advised that it would take steps to raise awareness amongst relevant staff to consider the requirements of section 81 of the TIA Act when completing log entries.

Paragraph 81(1)(g) requires the chief officer of an agency to cause to be recorded particulars of each occasion when, to the knowledge of an officer of the agency, lawfully intercepted information was given in evidence in a relevant proceeding in relation to the agency.

The Ombudsman identified large gaps (exceeding six months in some instances) between entries in the spreadsheet the ACIC uses to record each time lawfully intercepted information is used as evidence in a relevant proceeding. As such, the Ombudsman could not be confident that the register was complete and that ACIC was complying with paragraph 81(1)(g) of the TIA Act. The ACIC advised it had communicated this issue to relevant staff and reiterated the requirements of the TIA Act, directing staff to make accurate and timely records when intercepted information is used as evidence in proceedings.

Other issues noted under the Commonwealth Ombudsman's Telecommunications Interception Inspection Criteria

Under section 85 of the TIA Act, the Ombudsman may report on other contraventions of the TIA Act and do anything incidental or conducive to the performance of any of its functions under subsection 86(3). On this basis, the Ombudsman test the veracity of the records inspected under sections 80 and 81.

One of the Ombudsman's most important assessments is to check whether interceptions were conducted in accordance with warrants and whether the agency properly dealt with any intercepted information. In order to do this, the Ombudsman accessed agencies' systems to view the details of interceptions (when and what service was intercepted) and checked this against the warrant and other records agencies are required to keep under sections 80 and 81 of the TIA Act. As a result of conducting these checks the Ombudsman identified the following issues.

Unable to determine if intercepted internet data was authorised by the warrant

Section 7 of the TIA Act prohibits the interception of telecommunications except in certain instances, such as under a warrant. Section 63 of the TIA Act prevents a person from dealing with intercepted information obtained in contravention of section 7 of the TIA Act.

During each of the Ombudsman's two inspections at the ACIC and the AFP there were instances where the Ombudsman could not assess intercepted internet data due to the file type the carrier had provided. In turn, the Ombudsman could not confirm that the intercepted data was linked to the service specified on the warrant.

During the inspections period the Ombudsman made a suggestion to both the ACIC and the AFP that they implement measures to demonstrate that interceptions relating to internet data services can be linked to the service listed on the warrant. The ACIC advised that it is working with its interception platform vendor to rectify the issue, while the AFP advised it will consult other agencies and relevant carriers to identify solutions. The Ombudsman will follow this issue up at future inspections at the AFP and ACIC to assess what remedial action has been taken in order to achieve compliance with the TIA Act.

Interceptions made after the warrant was revoked

Under section 57 of the TIA Act, the chief officer of an agency may revoke a warrant at any time, and must do so if satisfied that the grounds on which the warrant was issued have ceased to exist. Section 58 of the TIA Act states that the chief officer must, on the revocation of a warrant, immediately take steps necessary to ensure that interceptions of communications under the warrant are discontinued.

At the Ombudsman's first inspections at both the ACIC and the AFP, the Ombudsman identified telecommunication interceptions that occurred after the relevant warrant had been revoked. At the Ombudsman's second inspection of the ACIC it disclosed two instances where telecommunications continued to be intercepted after the relevant warrants had been revoked. In all instances the agencies quarantined the affected data.

Other administrative issues

As part of the Ombudsman's inspection methodology the Ombudsman also reports on administrative errors which have resulted in non-compliance, including instances where the consequences may be negligible. At inspections the Ombudsman identified, and agencies disclosed, several administrative issues that resulted in non-compliance with requirements of the TIA Acts. These were:

- The AFP disclosed that the affidavit used in support of an application for two telecommunications service warrants did not include details of previous warrants. Paragraph 42(4)(a) of the TIA Act requires an affidavit supporting an application for a telecommunications service warrant to include details regarding the number of previous applications (if any) for warrants that the agency has made in relation to the service or person.
- One instance each at the ACIC and the AFP where notices required under section 59A were not provided to the Secretary of the Department of Home Affairs as soon as practicable, noting they were provided more than three months after the relevant events occurred.
- Multiple instances at the ACIC and the AFP where notifications and copies of warrants and revocations sent to the Secretary of the Department of Home Affairs were incorrectly addressed. The Ombudsman is satisfied that template changes at both agencies will resolve this issue.
- Shortcomings in section 94 reports to the Minister for Home Affairs, including ten instances where the report to the Minister under subsection 94(2) of the TIA Act was provided more than three months after the relevant warrant ceased to be in effect, and one instance where a section 94 report to the Minister incorrectly stated that no legally intercepted information was communicated externally under section 68 of the TIA Act.

The Ombudsman was satisfied these issues were the result of administrative errors and were not systemic in nature. The Ombudsman was also satisfied that those issues related to errors in templates or forms have been rectified to ensure future compliance.

Figure 5: Commonwealth Ombudsman's Telecommunications Interception Inspection Criteria

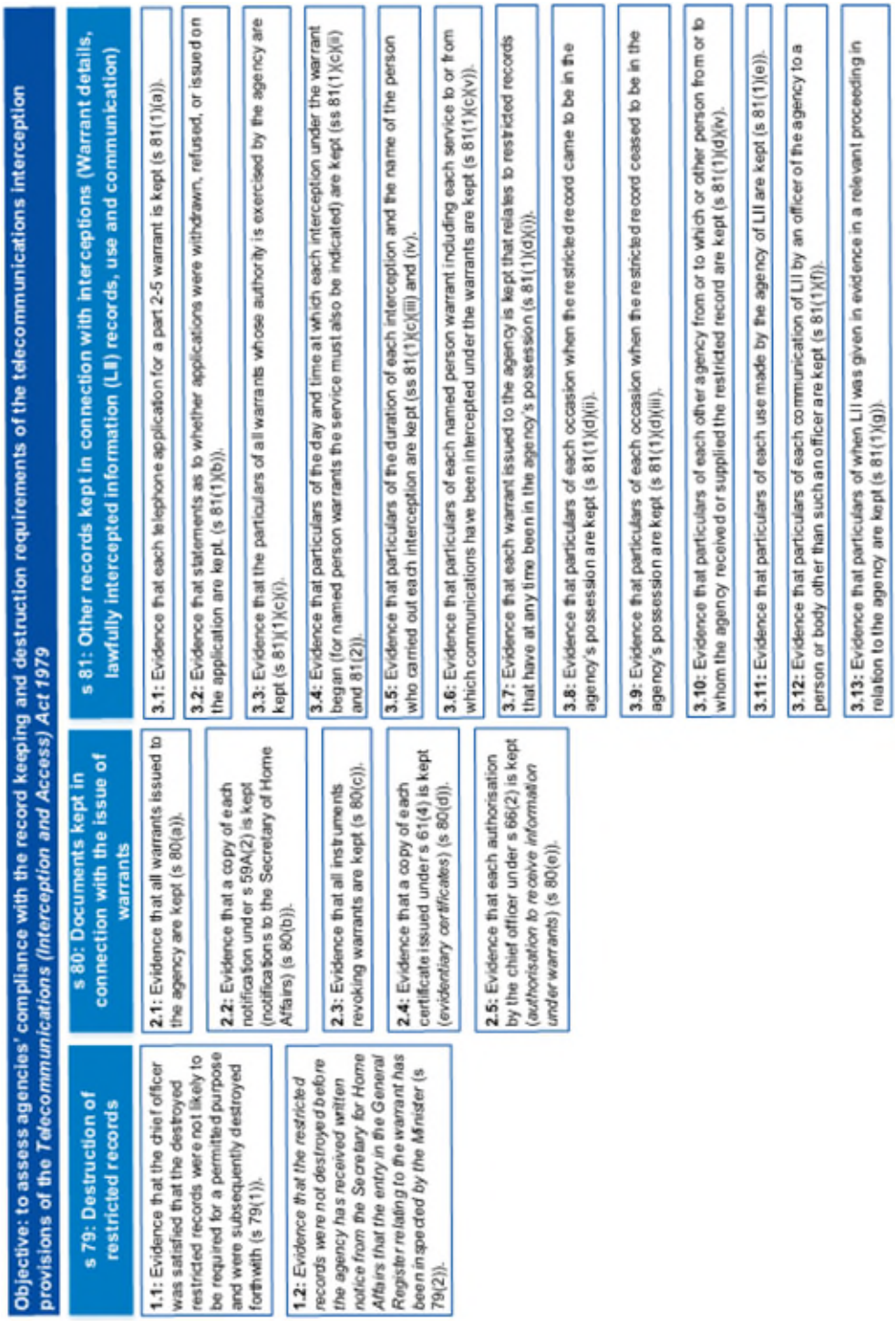
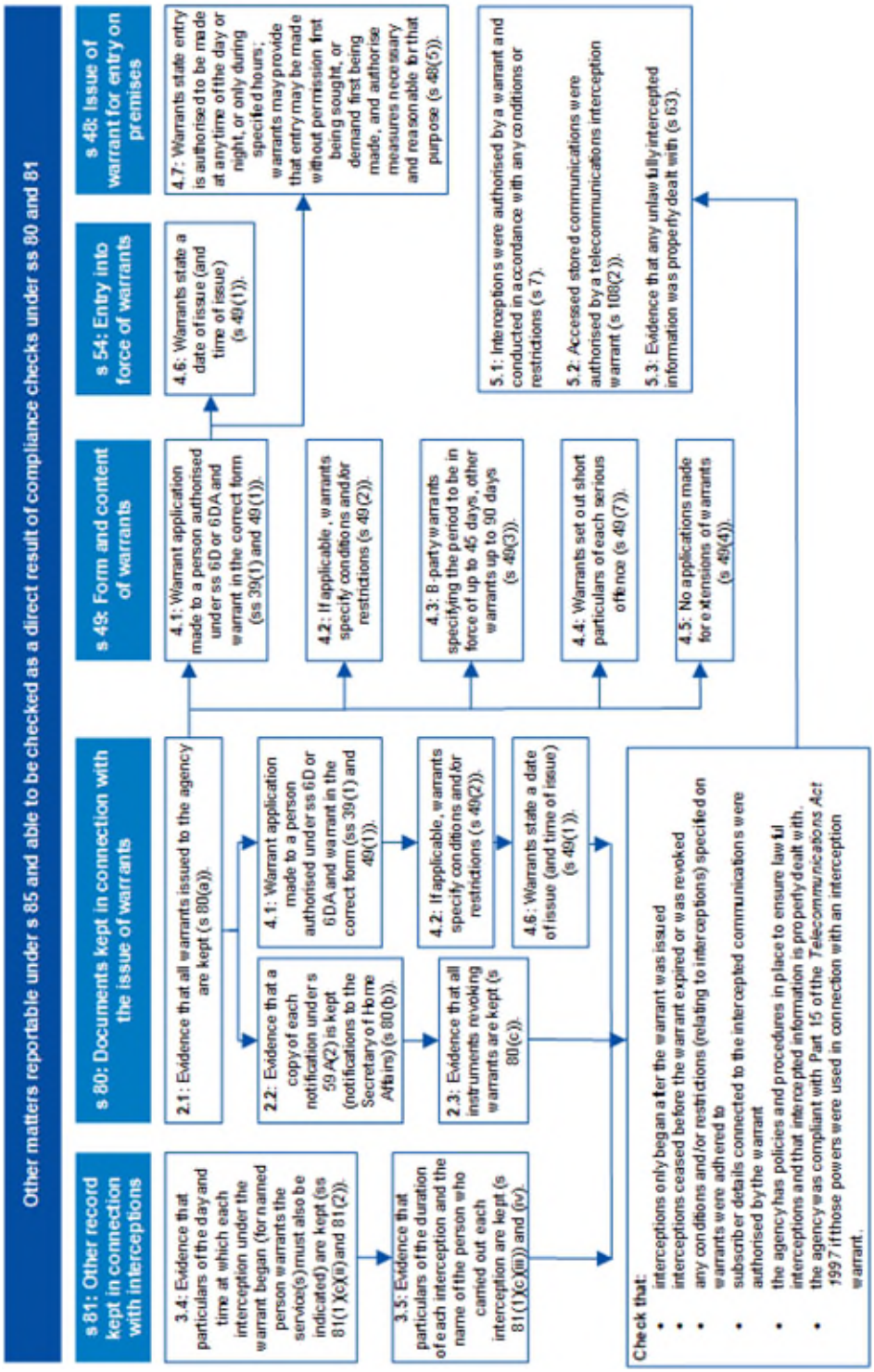


Figure 6: Other Matters reportable under section 85



CHAPTER 2 – STORED COMMUNICATIONS

Applications for stored communications warrants

Access to stored communications is regulated by Chapter 3 of the TIA Act. Chapter 3 of the TIA Act protects the privacy of people who use the Australian telecommunications network by making it an offence to access stored communications subject to limited lawful exceptions. The TIA Act prohibits stored communications from being accessed except as authorised under the circumstances prescribed in the TIA Act. Authorities and bodies that are 'criminal law-enforcement agencies' under the TIA Act can apply to an independent issuing authority[11] for a stored communications warrant to investigate a 'serious contravention'[12] 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 Home Affairs, ASIC, and the ACCC. Only criminal law-enforcement agencies are eligible to apply under Chapter 3 for a stored communications warrant

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 ($37,800 during the reporting period) for individuals or 900 penalty units ($189,000 during the reporting period) for non-individuals such as corporations.

Paragraphs 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 2019–20, 1,385 stored communications warrants were issued, representing an increase of 132 from the 1,253 warrants issued in the 2018–19 period.

[11] An issuing authority refers to the judicial or ministerial authority that has the power and is responsible for scrutinising applications for warrants under the TIA Act. An issuing authority may refuse a warrant application, approve and issue a warrant application, or impose additional conditions on a warrant application before approving.
[12] The latest penalty unit figures can be found at: www.asic.gov.au/about-asic/asic-investigations-and-enforcement/fines-and-penalties/

Table 23: Applications, telephone applications and renewal applications for stored communications warrants – paragraphs 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	
		18/19	19/20	18/19	19/20	18/19	19/20
ACCC	Made	9	12	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	9	12	-	-	-	-
ACIC	Made	2	2	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	2	2	-	-	-	-
ACLEI	Made	-	2	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	-	2	-	-	-	-
AFP	Made	100	67	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	100	67	-	-	-	-
CCC (WA)	Made	1	1	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	1	1	-	-	-	-
Home Affairs	Made	9	2	-	-	-	-
	Withdrawn	2	-	-	-	-	-
	Issued	7	2	-	-	-	-
IBAC	Made	3	1	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	3	1	-	-	-	-
ICAC (NSW)[13]	Made	7	2	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	7	2	-	-	-	-
ICAC (SA)	Made	-	-	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	-	-	-	-	-	-
LECC	Made	5	5	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	5	5	-	-	-	-
NSW CC	Made	1	3	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	1	3	-	-	-	-

[13] Correction for 2018-19: ICAC NSW figures relating to applications for and issuance of stored communications warrants have both been amended from 6 to 7 due to a reporting error in the 2018-19 Annual Report. As such, the total figures have also been amended.

Agency	Relevant statistics	Applications for stored communications warrants		Telephone applications for stored communications warrants		Renewal applications for stored communications warrants	
		18/19	19/20	18/19	19/20	18/19	19/20
NSW Police	Made	707	830	1	1	-	-
	Refused	-	-	-	-	-	-
	Issued	707	830	1	1	-	-
NT Police	Made	4	2	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	4	2	-	-	-	-
QLD CCC	Made	3	6	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	3	6	-	-	-	-
QLD Police	Made	165	173	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	165	173	-	-	-	-
SA Police	Made	26	34	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	26	34	-	-	-	-
TAS Police	Made	50	28	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	50	28	-	-	-	-
VIC Police	Made	115	112	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	115	112	-	-	-	-
WA Police	Made	48	103	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	48	103	-	-	-	-
TOTAL	**Made**	**1,255**	**1,385**	**1**	**1**	**0**	**0**
	Refused / Withdrawn	**2**	**0**	**0**	**0**	**0**	**0**
	Issued	**1,253**	**1,385**	**1**	**1**	**0**	**0**

Conditions or restrictions on stored communications warrants

Paragraph 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 24 presents this information. In 2019–20, 866 stored communications warrants were subject to conditions or restrictions, representing an increase of 133 compared to the 2018–19 period.

Table 24: Stored Communications warrants subject to conditions or restrictions – paragraph 162(2)(d)

Agency	18/19	19/20
ACCC	-	3
ICAC NSW[14]	1	-
NSW CC	1	-
NSW Police	707	830
QLD CCC	-	1
SA Police	24	32
TOTAL	**733**	**866**

Effectiveness of stored communications warrants

Paragraphs 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. The report must also set out how many proceedings, in which lawfully accessed information was given in evidence, ended during the reporting year.

Table 25 presents this information. In 2019–20, criminal law-enforcement agencies made 542 arrests, conducted 568 proceedings and obtained 298 convictions involving evidence obtained under stored communications warrants.

[14] Correction for 2018-19: ICAC NSW figures relating to conditions or restrictions on stored communications warrants have been amended from 0 to 1 due to a transposition error in the 2018-19 Annual Report. As such, the total figure has also been amended.

Table 25: Number of arrests, proceedings, and convictions made on the basis of lawfully accessed information – paragraphs 163(a)-(b)

Agency	Arrests		Proceedings		Convictions	
	18/19	19/20	18/19	19/20	18/19	19/20
ACIC	2	-	-	1	-	1
AFP	2	11	1	2	4	5
Home Affairs	2	-	-	-	-	-
NSW CC	-	1	-	-	-	-
NSW Police	383	313	843	539	227	246
NT Police	1	1	-	-	-	-
QLD CCC	7	-	-	-	-	-
QLD Police	108	139	14	7	14	7
SA Police	5	2	3	2	5	2
TAS Police	2	15	2	-	2	-
VIC Police	53	60	21	17	28	37
TOTAL	**565**	**542**	**884**	**568**	**280**	**298**

Care should be taken in interpreting Table 25 as an arrest recorded in one reporting period may not result in a prosecution (if any) until a later reporting period. Any resulting conviction may be recorded in that period, or an even later reporting period.

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 have 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.

Subsections 161A(1) and (2) of the TIA Act provide 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 26 presents this information. In 2019–20, 2,496 domestic preservation notices were given, an increase of 280 on the 2,216 given in 2018–19.

Table 26: Domestic preservation notices – subsection 161A(1)

Agency	Domestic preservation notices issued		Domestic preservation revocation notices issued	
	18/19	19/20	18/19	19/20
ACCC	12	27	3	7
ACIC	8	8	1	-
ACLEI	-	2	-	-
AFP	182	500	66	263
CCC (WA)	3	3	1	2
Home Affairs	10	16	1	13
IBAC	24	6	6	-
ICAC (NSW)	12	2	2	-
ICAC (SA)	11	1	6	1
LECC	8	9	-	1
NSW CC	1	4	-	1
NSW Police	909	977	180	145
NT Police	45	31	21	25
QLD CCC	25	38	6	11
QLD Police	373	343	136	90
SA Police	127	120	82	84
TAS Police	153	95	82	49
VIC Police	165	132	41	22
WA Police	148	182	89	97
TOTAL	**2,216**	**2,496**	**723**	**811**

Subsection 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 2019–20, the AFP reported that two foreign preservation notices were given, with four revocations.

Table 27: Foreign preservation notices – subsection 161A(2)

Agency	Foreign preservation notices given		Foreign preservation revocation notices given	
	18/19	19/20	18/19	19/20
AFP	10	2	2	4

International assistance

International assistance applications relate to international offences and are applications for a stored communications warrant made as a result of an authorisation under section:

(a) 15B of the *Mutual Assistance in Criminal Matters Act 1987*; or

(b) 78A of the *International Criminal Court Act 2002*; or

(c) 34A of the *International War Crimes Tribunals Act 1995*.

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.

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

Table 28 presents this information. In 2019–20, the AFP was the only agency to make applications for a stored communications warrant as a result of an international assistance application, totalling 12 applications.

Table 28: Applications for stored communications warrants as a result of international assistance applications – paragraph 162(1)(c)

Agency	Relevant statistics	Applications for stored communications warrants	
		18/19	19/20
AFP	Made	-	12
	Refused	-	-
	Issued	-	12
TOTAL	**Made**	**-**	**12**
	Refused	**-**	**-**
	Issued	**-**	**12**

Paragraph 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.

The AFP applied for and was issued 12 stored communications warrants on behalf of other countries in relation to international offences of the following nature:

- International money laundering – Part 10.2 – Division 400 – *Criminal Code Act 1995* or against Part 10.2 of the *Criminal Code Act 1995* (Money Laundering)
- Conspiracy – an offence against Part 11.5 of the *Criminal Code Act 1995*
- Computer Fraud – Sections 477.1 and/or 477.2 and/or 477.3 – *Criminal Code Act 1995*
- Fraud by wire radio or television – Section 474.14 – *Criminal Code Act 1995*

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

In 2019–20, there were four occasions in which lawfully accessed information or stored communications warrant information was provided to a foreign country, and zero occasions for provision to the International Criminal Court or a War Crimes Tribunal.

Ombudsman inspection report

The Commonwealth Ombudsman inspects the preservation notices and stored communications access records 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 for Home Affairs.

The Minister for Home Affairs 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 inspection report is received. 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.[15]

Definition

In 2019–20 the category of **'enforcement agency'** was restricted to the 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 Home Affairs, ASIC, and the ACCC.

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 a *criminal law-enforcement agency* can authorise the disclosure of prospective data when disclosure is considered to be reasonably necessary for the investigation of an offence punishable by imprisonment for at least three years. A prospective data authorisation comes into force once the relevant telecommunications service provider receives the request and is effective for 45 days or less.

[15] NT Police identified corrections regarding historic telecommunications data for the 2017–18 and 2018–19 reporting periods. The tables in this chapter include amended NT Police figures and amended totals as relevant for 2018–19. Appendix D provides both the original figures reported for the 2017–18 period and the 2018–19 period, and the amended figures as identified and corrected.

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.

Paragraph 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 29 provides this information. In 2019–20, 306,995 authorisations were made by agencies under section 178, an increase of 17,358 from the 289,637 authorisations made in 2018–19.

Table 29: Number of authorisations made by an enforcement agency for access to existing information or documents in the enforcement of a criminal law – paragraph 186(1)(a)

Agency	Authorisations	
	18/19	19/20
ACCC	100	123
ACIC	6,536	5,249
ACLEI	393	263
AFP	16,818	18,534
ASIC	1,800	1,432
CCC (WA)	122	207
Home Affairs	3,283	3,214
IBAC	539	473
ICAC (NSW)	298	175
ICAC (SA)	220	196
LECC	459	829
NSW CC	3,323	4,734
NSW Police	105,199	116,968
NT Police[16]	1,827	1,834
QLD CCC	1,009	710
QLD Police	23,693	25,221
SA Police	5,477	6,229
TAS Police	7,759	5,566
VIC Police	87,680	88,526
WA Police	23,102	26,512
TOTAL	**289,637**	**306,995**

[16] NT Police identified corrections for the 2018–19 period. The amended figures as identified and corrected are included in this table. Appendix D provides both the original figures reported for the 2018–19 period, and the amended figures as identified and corrected.

Existing data – assist in locating a missing person

Section 178A of the TIA Act provides that an authorised officer of the AFP 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.

Paragraph 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 30 presents this information. In 2019–20, 3,028 authorisations were made by agencies under section 178A, an increase of 454 from the 2,574 authorisations made in 2018–19.

Table 30: Number of authorisations made for access to existing information or documents for the location of missing persons – paragraph 186(1)(aa)

Agency	Authorisations	
	18/19	19/20
AFP	194	159
NSW Police	1,228	1,684
NT Police[17]	16	15
QLD Police	199	234
SA Police	79	63
TAS Police	168	78
VIC Police	447	561
WA Police	243	234
TOTAL	**2,574**	**3,028**

[17] NT Police identified corrections for the 2018–19 period. The amended figures as identified and corrected are included in this table. Appendix D provides both the original figures reported for the 2018–19 period, and the amended figures as identified and corrected.

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. Paragraph 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 31 presents this information. In 2019–20, 1,289 authorisations were made by agencies under section 179, a decrease of 459 from the 1,748 authorisations made in 2018–19.

Table 31: 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 – paragraph 186(1)(b)

Agency	Authorisations	
	18/19	19/20
ACCC	8	1
AFP	72	22
ASIC	39	42
Home Affairs	38	65
NSW Police	1,206	1,137
NT Police[18]	0	6
QLD CCC	5	1
QLD Police	3	-
TAS Police	374	10
WA Police	3	5
TOTAL	**1,748**	**1,289**

[18] NT Police identified corrections for the 2018–19 period. The amended figures as identified and corrected are included in this table. Appendix D provides both the original figures reported for the 2018–19 period, and the amended figures as identified and corrected.

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.

Paragraph 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 32. 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 2019–20, 32,856 prospective authorisations were made by agencies under section 180, an increase of 5,085 on the 27,771 authorisations made in 2018–19.

Table 32: Prospective data authorisations – paragraph 186(1)(c)

Agency	Number of authorisations made		Days specified in force		Actual days in force		Authorisations discounted	
	18/19	19/20	18/19	19/20	18/19	19/20	18/19	19/20
ACIC	1,279	1,086	39,671	39,982	29,938	28,063	35	75
ACLEI	88	34	3,960	1,530	3,748	1,462	-	-
AFP[19]	4,707	4,835	195,466	204,749	108,218	127,576	302	424
ASIC	37	25	119	74	116	72	-	-
CCC (WA)	63	94	2,829	4,183	2,137	3,043	7	6
Home Affairs	225	296	523	623	504	596	3	6
IBAC	310	267	13,776	11,390	10,858	8,724	33	35
ICAC (NSW)	75	31	3,323	1,369	2,848	1,300	-	2
ICAC (SA)	25	21	962	921	841	709	6	-
LECC	65	90	2,925	3,986	2,449	3,213	7	14
NSW CC	1,176	1,712	50,402	71,376	43,226	62,300	147	181
NSW Police	1,062	1,360	22,691	33,643	16,567	23,734	73	124
NT Police[20]	258	248	9,608	10,216	7,430	8,359	14	4
QLD CCC	210	152	8,540	5,945	6,351	4,448	8	10
QLD Police	4,252	4,199	185,008	181,427	138,986	121,723	342	555
SA Police	422	468	14,759	13,583	11,036	8,692	26	29
TAS Police	178	115	8,010	5,175	4,481	3,577	1	5
VIC Police	11,219	14,801	496,658	186,970	367,965	166,178	1,253	551
WA Police	2,120	3,022	75,812	119,310	74,877	105,770	224	318
TOTAL	**27,771**	**32,856**	**1,135,042**	**896,452**	**832,576**	**679,539**	**2,481**	**2,339**

Table 33 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 2019–20.

[19] The AFP has identified a correction for the 2017–18 reporting period relating to the number of prospective authorisations given in that reporting period. Appendix D provides both the original figures reported for the 2017–18 period, and the amended figures identified and amended by the AFP.
[20] NT Police identified corrections for the 2018–19 period. The amended figures as identified and corrected are included in this table. Appendix D provides both the original figures reported for the 2018–19 period, and the amended figures as identified and corrected.

Table 33: Average specified and actual time in force of prospective data authorisations

Agency	Average period specified		Average period actual	
	18/19	19/20	18/19	19/20
ACIC	31	37	24	28
ACLEI	45	45	43	43
AFP	42	42	25	29
ASIC	3	3	3	3
CCC (WA)	45	45	38	35
Home Affairs	2	2	2	2
IBAC	44	43	39	38
ICAC (NSW)	44	44	38	45
ICAC (SA)	38	44	44	37
LECC	45	44	42	42
NSW CC	43	42	42	41
NSW Police	21	25	17	19
NT Police[21]	37	41	30	34
QLD CCC	41	39	31	31
QLD Police	44	43	36	33
SA Police	35	29	28	20
TAS Police	45	45	25	33
VIC Police[22]	44	13	37	12
WA Police	36	39	39	39
AVERAGE	**36**	**35**	**31**	**30**

[21] NT Police identified corrections for the 2018–19 period. The amended figures as identified and corrected are included in this table. Appendix D provides both the original figures reported for the 2018–19 period, and the amended figures as identified and corrected.
[22] VIC Police has advised that the average period specified and actual for prospective data authorisations in 2019–20 differs from that in 2018–19 due to a change of administrative process whereby durations were set as a default to seven days rather than 45 days.

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.[23] 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*.

Paragraphs 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.

In 2019–20, the AFP made 66 authorisations under sections 180A, 180B, 180C and 180D of the TIA Act.

Following these authorisations, the AFP made 16 disclosures to foreign law enforcement agencies. Information was disclosed to the following countries: Argentina (one); Austria (one); France (one); New Zealand (two); Singapore (one); Sri Lanka (one); Switzerland (two); Taiwan (two); United Kingdom (two); United States of America (three).

Offences for which authorisations were made

Paragraph 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 34, 35, 36 and 37.

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.

[23] The AFP has identified a correction for the 2017–18 reporting period relating to the number of foreign prospective authorisations given in that reporting period. Appendix D provides both the original figures reported for the 2017–18 period, and the amended figures identified and amended by the AFP.

Table 34: Offences for which authorisations were made under section 178 to access existing data to enforce the criminal law – paragraph 186(1)(e)[24]

Categories of offences	ACCC	ACIC	ACLEI	AFP	ASIC	CCC (WA)	Home Affairs	IBAC	ICAC (NSW)	ICAC (SA)	LECC	NSW CC	NSW Police	NT Police	QLD CCC	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Abduction	-	-	-	414	-	-	-	-	-	-	-	36	10,017	90	3	1,217	340	445	2,908	4,197	**19,667**
Acts – injury	-	-	-	148	-	-	-	5	-	1	-	-	5,694	13	-	16	144	191	2,852	1,032	**10,096**
Bribery or corruption	-	-	263	54	-	204	5	461	27	160	523	1	1	6	-	3	45	-	67	400	**2,220**
Cartel offences	117	-	-	-	-	-	-	-	-	-	-	-	10	-	-	-	-	-	-	-	**127**
Conspire	-	-	-	46	4	-	-	-	-	-	-	-	53	-	-	-	8	-	258	35	**404**
Cybercrime	-	82	-	791	19	-	-	-	-	-	1	-	3,106	43	-	1,170	12	73	1,386	269	**6,952**
Dangerous acts	-	-	-	61	-	-	-	-	-	-	-	-	1,052	47	-	1,019	403	-	2,682	400	**5,664**
Fraud	6	-	-	1,520	382	2	1,346	3	119	35	10	425	15,452	83	445	602	568	386	9,728	1,715	**32,827**
Homicide	-	-	-	556	-	-	-	-	-	-	-	317	12,739	158	-	1,779	853	541	6,282	591	**23,816**
Illicit drug offences	-	265	-	8,518	-	-	1,502	-	-	-	78	3,402	29,498	959	184	4,740	1,848	2,019	17,990	7,139	**78,142**
Loss of life	-	-	-	5	-	1	-	-	-	-	-	-	820	1	-	637	41	1	412	1	**1,919**
Miscellaneous	-	-	-	220	1,076	-	54	-	-	-	-	10	4,554	60	79	7,420	31	102	118	422	**14,146**
Justice procedures	-	-	-	344	5	-	-	4	29	-	190	7	526	5	-	-	47	146	2,466	573	**4,342**
Organised offences	-	-	-	538	-	-	-	-	-	-	-	-	1,257	17	-	4	13	-	88	953	**2,870**
Pecuniary penalty	-	-	-	14	-	-	-	-	-	-	-	-	964	1	-	-	-	-	-	-	**979**
Public revenue	-	-	-	3	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	66	**69**

[24] Appendix E 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	NSW CC	NSW Police	NT Police	QLD CCC	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
People smuggling	-	-	-	279	-	-	57	-	-	-	-	-	1	-	-	-	-	-	-	2	**339**
Weapons	-	3	-	161	-	-	224	-	-	-	-	77	1,746	6	-	37	91	46	1,661	51	**4,103**
Property damage	-	-	-	122	-	-	-	-	-	-	-	-	1,524	16	-	-	158	-	1,996	10	**3,826**
Public order offences	-	-	-	3	-	-	-	-	-	-	-	-	167	-	-	24	6	-	260	60	**520**
Robbery	-	-	-	317	-	-	-	-	-	-	-	19	10,845	43	-	1,816	669	276	8,503	2,346	**24,834**
Serious damage	-	-	-	13	-	-	-	-	-	-	-	80	413	12	-	568	69	141	2	228	**1,526**
Sexual assault	-	-	-	2,748	-	-	-	-	-	-	27	-	7,607	167	-	769	552	200	5,180	1,211	**18,461**
Special ACC Investigation	-	4,899	-	-	-	-	-	-	-	-	-	-	-	-	-	99	-	-	-	1	**4,999**
Terrorism offences	-	-	-	1,097	-	-	-	-	-	-	-	358	298	-	-	-	22	-	451	122	**2,348**
Theft	-	-	-	344	-	-	78	-	-	-	-	2	5,879	41	-	1,321	393	532	8,796	1,185	**18,571**
Traffic	-	-	-	16	-	-	-	-	-	-	-	-	801	6	-	274	12	38	1,048	224	**2,419**
Unlawful entry	-	-	-	202	-	-	-	-	-	-	-	-	1,944	22	-	1,469	318	432	13,392	3,279	**21,058**
TOTAL	**123**	**5,249**	**263**	**18,534**	**1,486**	**207**	**3,266**	**473**	**175**	**196**	**829**	**4,734**	**116,968**	**1,796**	**711**	**24,984**	**6,643**	**5,569**	**88,526**	**26,512**	**307,244**

Table 35: Offences against which authorisations were made under section 178A for access to existing data to locate a missing person – paragraph 186(1)(e)[25]

Categories of offences	AFP	NSW Police	NT Police	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Abduction	-	18	-	2	-	-	-	-	**20**
Acts – injury	-	1	-	-	-	-	-	-	**1**
Bribery or corruption	-	-	-	-	-	-	-	-	**-**
Cartel offences	-	-	-	-	-	-	-	-	**-**
Conspire	-	-	-	-	-	-	-	-	**-**
Cybercrime	-	-	-	1	-	-	-	-	**1**
Dangerous acts	-	1	-	-	-	-	-	-	**1**
Fraud	-	-	-	-	-	-	-	-	**-**
Homicide	-	15	-	4	-	-	-	-	**19**
Illicit drug offences	-	-	-	7	-	-	-	-	**7**
Loss of life	-	34	2	1	-	-	-	-	**37**
Miscellaneous	-	2	13	16	-	-	-	-	**31**
Justice procedures	-	2	-	-	-	-	-	-	**2**
Organised offences	-	-	-	-	-	-	-	-	**-**
Pecuniary penalty	-	-	-	-	-	-	-	-	**-**
Public revenue	-	-	-	-	-	-	-	-	**-**

[25] 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	NSW Police	NT Police	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
People smuggling	-	-	-	-	-	-	-	-	**-**
Weapons	-	-	-	-	-	-	-	-	**-**
Property damage	-	-	-	-	-	-	-	-	**-**
Public order offences	-	1	-	-	-	-	-	-	**1**
Robbery	-	-	-	2	-	-	-	-	**2**
Serious damage	-	-	-	-	-	-	-	-	**-**
Sexual assault	-	-	-	1	-	-	-	-	**1**
Special ACC Investigation	-	-	-	-	-	-	-	-	**-**
Terrorism offences	-	-	-	-	-	-	-	-	**-**
Theft	-	-	-	1	-	-	-	-	**1**
Traffic	-	-	-	-	-	-	-	-	**-**
Unlawful entry	-	-	-	5	-	-	-	-	**5**
No offence attached to s178A authorisation	159	1,610	15	194	63	78	561	234	**2,914**
TOTAL	**159**	**1,684**	**30**	**234**	**63**	**78**	**561**	**234**	**3,043**

Table 36: 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 – paragraph 186(1)(e)

Categories of offences	ACCC	AFP	ASIC	Home Affairs	NSW Police	NT Police	QLD CCC	TAS Police	WA Police	TOTAL
Abduction	-	-	-	-	69	-	-	-	-	**69**
Acts – injury	-	-	-	-	30	-	-	-	-	**30**
Bribery or corruption	-	-	-	-	-	-	-	-	-	**-**
Cartel offences	-	-	-	-	-	-	-	-	-	**-**
Conspire	-	-	-	-	-	-	-	-	-	
Cybercrime	-	1	-	-	20	-	-	-	-	**21**
Dangerous acts	-	1	-	-	69	-	-	-	-	**70**
Fraud	-	2	32	38	69	-	-	-	-	**141**
Homicide	-	-	-	-	49	-	-	-	-	**49**
Illicit drug offences	-	2	-	19	125	-	-	-	-	**146**
Loss of life	-	-	-	-	23	-	-	-	-	**23**
Miscellaneous	-	-	17	-	29	4	1	3	1	**55**
Justice procedures	-	-	-	-	2	2	-	-	-	**4**
Organised offences	-	-	-	-	70	-	-	-	-	**70**
Pecuniary penalty	1	7	2	3	202	-	-	-	-	**215**
Public revenue	-	8	-	-	-	-	-	-	-	**8**
People smuggling	-	-	-	-	-	-	-	-	-	**-**

Categories of offences	ACCC	AFP	ASIC	Home Affairs	NSW Police	NT Police	QLD CCC	TAS Police	WA Police	TOTAL
Weapons	-	-	-	5	3	-	-	6	-	**14**
Property damage	-	-	-	-	4	-	-	-	-	**4**
Public order offences	-	-	-	-	2	-	-	-	-	**2**
Robbery	-	-	-	-	242	-	-	-	-	**242**
Serious damage	-	-	-	-	-	-	-	-	-	**-**
Sexual assault	-	-	-	-	34	-	-	-	-	**34**
Special ACC Investigation	-	-	-	-	-	-	-	-	-	**-**
Terrorism offences	-	1	-	-	-	-	-	-	-	**1**
Theft	-	-	-	-	63	-	-	-	-	**63**
Traffic	-	-	-	-	22	-	-	1	4	**27**
Unlawful entry	-	-	-	-	10	-	-	-	-	**10**
TOTAL	**1**	**22**	**51**	**65**	**1,137**	**6**	**1**	**10**	**5**	**1,298**

Table 37: 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 – paragraph 186(1)(e)

Categories of offences	ACIC	ACLEI	AFP	ASIC	CCC (WA)	Home Affairs	IBAC	ICAC (NSW)	ICAC (SA)	LECC	NSW CC	NSW Police	NT Police	QLD CCC	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Abduction	-	-	23	-	-	-	-	-	-	-	7	79	5	3	238	33	5	606	74	**1,073**
Acts – injury	-	-	20	-	-	-	-	-	-	-	-	140	4	-	44	43	-	841	129	**1,221**
Bribery or corruption	-	34	6	-	94	4	258	14	21	60	-	-	-	11	4	-	-	32	11	**549**
Cartel offences	-	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	-	-	**1**
Conspire	-	-	13	-	-	-	-	-	-	-	-	2	-	-	14	-	1	43	8	**81**
Cybercrime	66	-	162	-	-	-	-	-	-	-	-	2	-	-	15	2	-	49	-	**296**
Dangerous acts	-	-	1	-	-	-	-	-	-	-	-	2	4	-	18	13	-	363	3	**404**
Fraud	-	-	229	25	-	179	-	17	-	2	133	36	3	76	107	1	1	563	180	**1,552**
Homicide	-	-	53	-	-	-	-		-	-	80	52	2	-	288	32	18	706	40	**1,271**
Illicit drug offences	163	-	2,846	-	-	55	-	-	-	17	1,302	652	215	35	2,591	202	59	3,381	1,453	**12,971**
Loss of life	-	-	7	-	-	-	-	-	-	-	-	16	-	-	26	1	-	8	-	**58**
Miscellaneous	-	-	35	-	-	-	-	-	-	-	6	42	1	26	46	17	6	26	58	**263**
Justice procedures	-	-	72	-	-	-	9	-	-	10	3	5	-	-	-	1	3	917	-	**1,020**
Organised offences	-	-	761	-	-	-	-	-	-	-	-	6	-	-	-	2	-	2	-	**771**
Pecuniary penalty	-	-	3	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**3**
Public revenue	-	-	4	-	-	-	-	-	-	-	-	4	-	-	-	-	-	2	-	**10**

Categories of offences	ACIC	ACLEI	AFP	ASIC	CCC (WA)	Home Affairs	IBAC	ICAC (NSW)	ICAC (SA)	LECC	NSW CC	NSW Police	NT Police	QLD CCC	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
People smuggling	-	-	41	-	-	2	-	-	-	-	-	-	-	-	-	-	-	-	-	**43**
Weapons	12	-	91	-	-	54	-	-	-	-	34	85	-	-	115	17	-	546	12	**966**
Property damage	-	-	1	-	-	-	-	-	-	-	-	9	5	-	1	-	-	187	1	**204**
Public order offences	-	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	2	89	-	**92**
Robbery	-	-	77	-	-	-	-	-	-	-	8	92	6	-	253	42	7	1,234	241	**1,960**
Serious damage	-	-	1	-	-	-	-	-	-	-	19	5	2	-	19	1	-	17	39	**103**
Sexual assault	-	-	115	-	-	-	-	-	-	1	1	34	1	-	44	13	2	419	29	**659**
Special ACC Investigation	848	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**848**
Terrorism offences	-	-	133	-	-	-	-	-	-	-	118	-	-	-	1	1	-	41	119	**413**
Theft	-	-	98	-	-	-	-	-	-	-	-	68	-	-	162	4	5	1,937	180	**2,454**
Traffic	-	-	10	-	-	-	-	-	-	-	-	2	-	-	-	4	-	112	6	**134**
Unlawful entry	-	-	31	-	-	-	-	-	-	-	-	25	2	-	213	39	6	2,680	439	**3,435**
TOTAL	**1,089**	**34**	**4,833**	**25**	**94**	**294**	**267**	**31**	**21**	**90**	**1,711**	**1,360**	**250**	**151**	**4,199**	**468**	**115**	**14,801**	**3,022**	**32,855**

Age of data under disclosure

Paragraph 186(1)(f) and subsection 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 38 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 2019–20, 84 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,[26] 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.

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

Table 38: Periods for which retained data was held by carrier before authorised disclosure – paragraph 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	4	9	23	6	8	9	14	3	48	**124**
ACIC	4,341	450	254	64	74	19	11	2	34	**5,249**
ACLEI	164	30	18	21	6	1	-	4	19	**263**
AFP	12,506	2,277	940	969	465	205	164	262	927	**18,715**
ASIC	1,327	25	42	13	1	4	9	10	43	**1,474**
CCC (WA)	277	1	1	1	-	1	4	-	16	**301**
Home Affairs	2,625	425	200	105	70	33	24	10	77	**3,569**
IBAC	407	21	13	7	2	-	5	3	15	**473**
ICAC (NSW)	75	14	8	3	3	8	3	1	60	**175**
ICAC (SA)	76	36	25	6	6	1	1	5	40	**196**
LECC	591	39	73	48	14	15	5	2	42	**829**
NSW CC	3,556	341	159	213	99	36	11	104	215	**4,734**
NSW Police	103,685	6,008	3,248	1,593	1,622	976	376	368	1,913	**119,789**
NT Police	1,671	98	50	23	3	3	2	5	12	**1,867**
QLD CCC	626	56	36	23	49	9	4	2	58	**863**
QLD Police	20,552	1,771	1,027	568	397	266	188	135	549	**25,453**
SA Police	4,060	786	427	321	151	103	70	59	335	**6,312**
TAS Police	4,646	452	193	74	68	27	35	10	152	**5,657**
VIC Police	82,505	3,285	1,284	702	377	126	177	104	527	**89,087**
WA Police	19,564	2,098	1,360	817	781	401	263	145	1,312	**26,741**
TOTAL	**263,258**	**18,222**	**9,381**	**5,577**	**4,196**	**2,243**	**1,366**	**1,234**	**6,394**	**311,871**

Types of retained data

Paragraphs 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 subsection 187AA(1). Data within item 1 of that subsection is typically considered 'subscriber data' and includes information identifying the user of a telecommunications service. Data within items 2–6 of that subsection are typically considered 'traffic data' and include information such as the time, duration, and source of a communication.[27]

Table 39: Types of retained data disclosed in authorisations – paragraphs 186(1)(g) and 186(1)(h)

Agency	Item 1: subscriber data	Items 2 – 6: traffic data	TOTAL
ACCC	55	69	**124**
ACIC	3,327	1,922	**5,249**
ACLEI	133	130	**263**
AFP	14,689	4,026	**18,715**
ASIC	1,309	165	**1,474**
CCC (WA)	156	51	**207**
Home Affairs	2,618	1,266	**3,884**
IBAC	355	135	**490**
ICAC (NSW)	102	73	**175**
ICAC (SA)	78	118	**196**
LECC	592	237	**829**
NSW CC	2,335	2,399	**4,734**
NSW Police	87,372	32,417	**119,789**
NT Police	1,465	390	**1,855**
QLD CCC	658	205	**863**
QLD Police	18,203	5,407	**23,610**
SA Police	3,903	2,409	**6,312**
TAS Police	4,817	840	**5,657**
VIC Police	64,493	24,594	**89,087**
WA Police	20,857	5,984	**26,841**
TOTAL	**227,517**	**82,837**	**310,354**

[27] Appendix F further explains the type of data included in items 1–6 of the table at subsection 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.

Paragraphs 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 40 and 41 present this information. In 2019–20, one historical data authorisation was made under one JIW issued to the QLD CCC for the enforcement of the criminal law.

Table 40: Journalist information warrants issued – paragraph 186(1)(j)

Agency	Warrants Issued	
	18/19	19/20
AFP	6	-
QLD CCC	-	1

Table 41: Number of authorisations made under journalist information warrants – paragraph 186(1)(i)

Agency	Authorisations made									
	18/19					19/20				
	s178	s78A	s179	s180	TOTAL	s178	s178A	s179	s180	TOTAL
AFP	20	-	-	-	**20**	-	-	-	-	**0**
QLD CCC	-	-	-	-	**0**	**1**	-	-	-	**1**

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 42).

Table 42 further sets out the costs recovered from criminal law-enforcement agencies for the purpose of complying with their data retention obligations.

Table 42: 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)
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
2019–20	$21,246,398.52	$11,165,966.50
TOTAL	**$238,274,916.41**	**$50,366,597.73**

The Data Retention Industry Grants Programme closed on 23 February 2016 with the last funding provided during the 2018–19 reporting period. As such, there was no funding provided under the Data Retention Industry Grants Programme in 2019–20.

CHAPTER 4 – INDUSTRY ASSISTANCE

Part 15 of the Telecommunications Act sets out an industry assistance framework providing 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 1 July 2019 and 30 June 2020.

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[28] 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 43: Eligible agencies under Part 15 of the Telecommunications Act

Agency	Industry assistance powers available to agencies		
	TAR	TAN	TCN
Interception Agencies[29]	✓	✓	✓
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.

[28] Categories of designated communications providers and their eligible activities are at Appendix G
[29] 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 offences against a law in force in a foreign country 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

Paragraphs 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 44. In 2019–20, eleven TARs were given by interception agencies to designated communications providers. One was given by the ACIC, three were given by the AFP, and seven were given by NSW Police. No TANs or TCNs were given by interception agencies.

Table 44: Number of Technical Assistance Requests, Technical Assistance Notices, and Technical Capability Notices given between 1 July 2019 and 30 June 2020 – paragraphs 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
ACIC	1	-	-	**1**
AFP[30]	3	-	-	**3**
NSW Police	7	-	-	**7**
TOTAL	**11**	**0**	**0**	**11**

Offences enforced through industry assistance

Paragraph 317ZS(1)(d) of the Telecommunications Act provides that if any TARs, TANs or TCNs are 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 2019–20 period.

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.[31]

[30] Two of the AFP's three TARS given in the 2019–20 reporting period were not given for specific offences, but rather were given to be used against all serious offences as the need arose. These two TARs were then revoked prior to assistance being utilised.
[31] Appendix F contains a description of each of the categories of offences.

Table 45: Kinds of serious Australian offences enforced through technical assistance requests – paragraph 317ZS(1)(d) of the Telecommunications Act 1997

Categories of offences	ACIC	AFP	NSW Police	TOTAL
Abduction offences	-	-	-	-
ACIC Investigation	-	-	-	-
Acts intended to cause injury	-	-	-	-
Bribery or corruption	-	-	-	-
Cartel offences	-	-	-	-
Conspire/aid/abet offences	-	-	-	-
Cybercrime offences	-	1	-	1
Dangerous acts endangering a person	-	-	-	-
Fraud and deception	-	-	-	-
Homicide	-	-	-	-
Illicit drug offences	1	-	6	7
Loss of life	-	-	-	-
Justice procedures	-	-	-	-
Organised offences	-	-	-	-
People smuggling	-	-	-	-
Weapons offences	-	-	-	-
Property damage	-	-	-	-
Public order offences	-	-	-	-
Robbery	-	-	1	1
Serious damage	-	-	-	-
Sexual assault	-	-	-	-
Telecommunications offences	-	-	-	-
Terrorism offences	-	-	-	-
Theft	-	-	-	-
Traffic offences	-	-	-	-
Unlawful entry	-	-	-	-
TOTAL	1	1	7	9

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 (IGIS), the Commonwealth Ombudsman or State and Territory oversight bodies.

The IGIS 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 IGIS 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 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 industry assistance measures complement these pre-existing TIA Act powers, this ensures the Commonwealth Ombudsman can oversight their collective 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 AFP 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 by responsible ministers and is reasonable, proportionate, practicable and technically feasible.

If requested 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 systemic vulnerability or 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.[32]

[32] Further information on Part 15 of the Telecommunications 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 TIA Act and Part 15 of the Telecommunications Act, 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 section 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 Force	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 Force	15 July 1997

APPENDIX C – CATEGORIES OF SERIOUS OFFENCES UNDER THE TIA ACT

Serious offence category	Offences covered
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 abuse 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)
Special ACC investigation	TIA Act, s 5D(1)(f)
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 D – UPDATED FIGURES FOR PREVIOUS REPORTING PERIODS

AFP 2017–18:

Upon compiling the figures for the 2019–20 period, the AFP identified a reporting error for the 2017–18 period. Specifically, the AFP received one prospective data request under paragraph 180B(2) which was subsequently extended under section 180B(6) of the TIA Act. This was reported as a domestic prospective authorisation in the 2017–18 report. The AFP has issued a correction, specifying that these authorisations should have been correctly recorded as two foreign prospective authorisations rather than one domestic prospective authorisation. The corrected figures are reported below:

Prospective data authorisations – paragraph 186(1)(c)

	Number of authorisations made		Days specified in force		Actual days in force		Authorisations discounted	
Agency	17/18 Original	17/18 Updated	17/18 Original	17/18 Updated	17/18 Original	17/18 Updated	17/18 Original	17/18 Updated
AFP	3,701	3,700	144,571	144,555	124,850	124,834	116	116
TOTAL	**23,947**	**23,946**	**911,437**	**911,421**	**740,514**	**740,498**	**2,347**	**2,347**

Number of authorisations made by the AFP under sections 180A, 180B, 180C and 180D of the TIA Act – paragraphs 186(1)(ca)–(cb) and subsection 186(2)

AFP	Authorisations	
	17/18 (updated figures as included in 18/19 report)	17/18 further updated (as identified in the 19/20 reporting period)
Number of authorisations	69	71
Disclosures made	Austria (one) Greece (two) India (one) Ireland (one) New Zealand (two) Singapore (one) Switzerland (one) United Kingdom (one) United States of America (three)	Austria (one) Greece (two) India (one) Ireland (one) New Zealand (two) Singapore (one) Switzerland (one) United Kingdom (one) United States of America (three)
TOTAL	**69 authorisations** **13 disclosures**	**71 authorisations** **13 disclosures**

NT Police 2017–18:

NT Police identified corrections regarding access to historic telecommunications data for the 2017–18 reporting period. Below details both the original figures provided for the 2017–18 report, and the amended figures as identified and corrected.

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

Agency	Authorisations	
	17/18 Original	17/18 Updated
NT Police	2,105	2,121
TOTAL	**295,779**	**295,795**

Prospective data authorisations – paragraph 186(1)(c)

	Number of authorisations made		Days specified in force		Actual days in force		Authorisations discounted	
Agency	17/18 Original	17/18 Updated	17/18 Original	17/18 Updated	17/18 Original	17/18 Updated	17/18 Original	17/18 Updated
NT Police	400	398	15,594	15,226	11,588	11,187	24	21
TOTAL	**23,947**	**23,945**	**911,437**	**911,069**	**740,514**	**740,113**	**2,347**	**2,344**

Average specified and actual time in force of prospective data authorisations

Agency	Average period specified		Average period actual	
	17/18 Original	17/18 Updated	17/18 Original	17/18 Updated
NT Police	39	38	31	30
TOTAL AVERAGE	**35**	**35**	**31**	**31**

Offences for which authorisations were made under section 178 to access existing data to enforce the criminal law – paragraph 186(1)(e)

Categories of offences	17/18 Original	17/18 Updated
Abduction	151	144
Acts - injury	20	18
Bribery or corruption	2	1
Cartel offences	-	-
Conspire	1	1
Cybercrime	65	58
Dangerous acts	57	56
Fraud	79	90
Homicide	113	130
Illicit drug offences	1,210	1,207

Categories of offences	17/18 Original	17/18 Updated
Loss of life	5	2
Miscellaneous	97	80
Justice procedures	10	2
Organised offences	3	3
Pecuniary penalty	-	-
Public revenue	-	-
People smuggling	-	-
Weapons	2	1
Property damage	4	5
Public order offences	-	-
Robbery	24	33
Serious damage	47	47
Sexual assault	126	146
Special ACC Investigation	-	-
Terrorism offences	2	2
Theft	53	55
Traffic	7	7
Unlawful entry	24	33
TOTAL	2,102	2,121

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 – paragraph 186(1)(e)

Categories of offences	17/18 Original	17/18 Updated
Abduction	11	7
Acts – injury	1	9
Bribery or corruption	8	6
Cartel offences	-	-
Conspire	-	-
Cybercrime	-	-
Dangerous acts	-	-
Fraud	6	5
Homicide	8	6
Illicit drug offences	341	327
Loss of life	1	-
Miscellaneous	3	2
Justice procedures	8	8
Organised offences	-	-
Pecuniary penalty	-	-
Public revenue	-	-
People smuggling	-	-
Weapons	-	-
Property damage	-	6
Public order offences	-	-
Robbery	2	1
Serious damage	4	2
Sexual assault	10	6
Special ACC Investigation	-	-
Terrorism offences	-	-

Categories of offences	17/18 Original	17/18 Updated
Theft	9	3
Traffic	-	-
Unlawful entry	6	10
TOTAL	**418**	**398**

Periods which retained data was held by carrier before authorised disclosure – paragraph 186(1)(f)

NT Police	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
17/18 Original	1,910	97	45	17	15	9	7	4	17	**2,121**
17/18 Updated	2,123	47	15	17	15	9	7	4	17	**2,254**

Types of retained data disclosed in authorisations – paragraphs 186(1)(g) and 186(1)(h)

NT Police	Item 1: subscriber data	Items 2 – 6: traffic data	TOTAL
17/18 Original	1,744	377	**2,121**
17/18 Updated	1,903	351	**2,254**

NT Police 2018–19:

NT Police also identified corrections for the 2018–19 period with respect to access and use of historical telecommunications data. Below are the original figures provided for the 2018–19 report, and the amended figures as identified and corrected by NT Police.

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

Agency	Authorisations	
	18/19 Original	18/19 Updated
NT Police	3,543	1,827
TOTAL	**291,353**	**289,637**

Offences against which authorisations were made under section 178A for access to existing data to locate a missing person – paragraph 186(1)(e)

Agency	Authorisations	
	18/19 Original	18/19 Updated
NT Police	31	16
TOTAL	**2,589**	**2,574**

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 – paragraph 186(1)(e)

Agency	Authorisations	
	18/19 Original	18/19 Updated
NT Police	1	0
TOTAL	**1,749**	**1,748**

Prospective data authorisations – paragraph 186(1)(c)

	Number of authorisations made		Days specified in force		Actual days in force		Authorisations discounted	
Agency	18/19 Original	18/19 Updated	18/19 Original	18/19 Updated	18/19 Original	18/19 Updated	18/19 Original	18/19 Updated
NT Police	311	258	9,661	9,608	7,528	7,430	14	14
TOTAL	**27,824**	**27,771**	**1,135,095**	**1,135,042**	**832,674**	**832,576**	**2,481**	**2,481**

Average specified and actual time in force of prospective data authorisations

Agency	Average period specified		Average period actual	
	18/19 Original	18/19 Updated	18/19 Original	18/19 Updated
NT Police	31	37	25	30
TOTAL AVERAGE	**36**	**36**	**30**	**31**

Offences for which authorisations were made under section 178 to access existing data to enforce the criminal law – paragraph 186(1)(e)

Categories of offences	18/19 Original	18/19 Updated
Abduction	270	148
Acts – injury	52	34
Bribery or corruption	2	1
Cartel offences	-	-
Conspire	1	-
Cybercrime	103	27
Dangerous acts	110	55

Categories of offences	18/19 Original	18/19 Updated
Fraud	148	65
Homicide	323	211
Illicit drug offences	1,838	901
Loss of life	-	4
Miscellaneous	119	113
Justice procedures	7	5
Organised offences	5	2
Pecuniary penalty	-	-
Public revenue	-	-
People smuggling	-	-
Weapons	2	1
Property damage	9	5
Public order offences	-	-
Robbery	80	49
Serious damage	54	11
Sexual assault	267	126
Special ACC Investigation	-	-
Terrorism offences	2	-
Theft	99	49
Traffic	8	1
Unlawful entry	46	19
TOTAL	**3,545**	**1,827**

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 – paragraph 186(1)(e)

Categories of offences	18/19 Original	18/19 Updated
Abduction	10	7
Acts – injury	4	3
Bribery or corruption	-	-
Cartel offences	-	-
Conspire	-	-
Cybercrime	-	-
Dangerous acts	2	2
Fraud	2	-
Homicide	7	6
Illicit drug offences	260	225
Loss of life	-	-
Miscellaneous	2	-
Justice procedures	-	-
Organised offences	-	-
Pecuniary penalty	-	-
Public revenue	-	-
People smuggling	-	-
Weapons	-	-
Property damage	-	-
Public order offences	-	-
Robbery	5	4
Serious damage	2	-
Sexual assault	12	6

Categories of offences	18/19 Original	18/19 Updated
Special ACC Investigation	-	-
Terrorism offences	-	-
Theft	4	4
Traffic	-	-
Unlawful entry	1	1
TOTAL	**311**	**258**

Periods which retained data was held by carrier before authorised disclosure – paragraph 186(1)(f)

NT Police	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
18/19 Original	3,267	67	23	34	18	12	15	8	52	**3,496**
18/19 Updated	1,769	25	10	20	4	3	9	5	42	**1,887**

Types of retained data disclosed in authorisations – paragraphs 186(1)(g) and 186(1)(h)

NT Police	Item 1: subscriber data	Items 2 – 6: traffic data	TOTAL
18/19 Original	3,008	667	**3,675**
18/19 Updated	1,552	335	**1,887**

APPENDIX E – 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 F – 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.	Paragraph 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.

	Item	Description of information	Explanation
4.	**The date, time and duration of a communication, or of its connection to a relevant service**	The date and time (including the time zone) of the following relating to the communication (with sufficient accuracy to identify the communication): 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.
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 paragraph 187A(4)(c).

	Item	Description of information	Explanation
6.	**The location of equipment or a line used in connection with a communication**	The following in relation to the equipment or line used to send or receive the communication: 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. Paragraph 187(4)(e) of the TIA 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 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
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

www.homeaffairs.gov.au