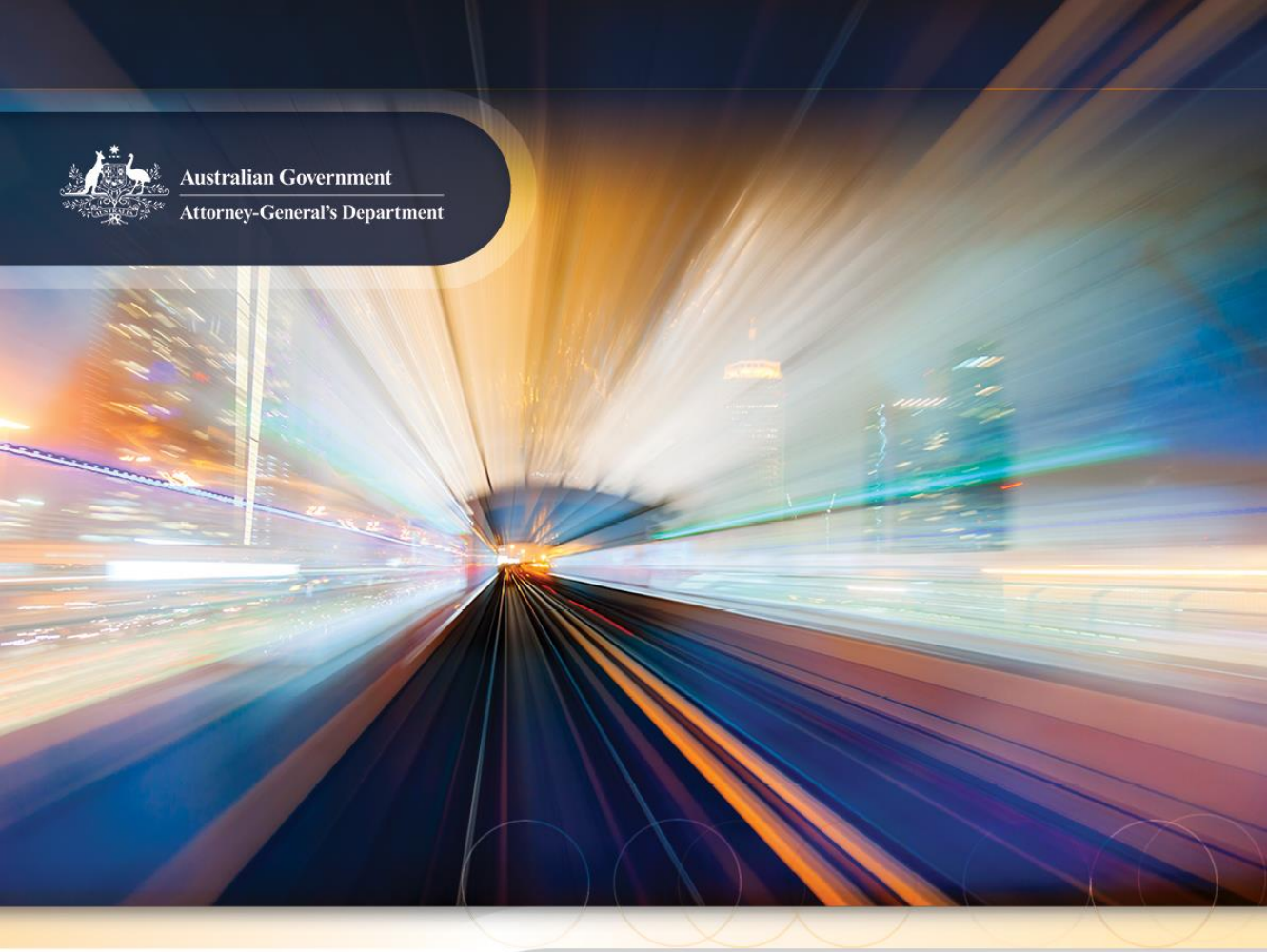


Australian Government
Attorney-General's Department

2021-22 Annual Report under the *Telecommunications (Interception and Access) Act 1979* and Part 15 of *Telecommunications Act 1997*

ISSN: 2653-7974 (Print)
ISSN: 2653-7982 (Online)

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

Electronic Surveillance Section
Attorney-General's Department
3-5 National Circuit
BARTON ACT 2600

2021-22 Annual Report

under the

Telecommunications (Interception and Access) Act 1979

and

Part 15 of the *Telecommunications Act 1997*

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)
CSNSW	Corrective Services New South Wales
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

KEY STATISTICS

The following key statistics are relevant to 2021-22:

- There were 3,207 interception warrants that were issued to 16 interception agencies. This was a decrease of 274 on the 3,481 issued in 2020-21.
- There were six applications for interception warrants that were refused. This decreased by one compared to 2020-21.
- The majority of serious offences that were specified in interception warrants issued were serious drug offences and/or trafficking (1,508 times), followed by murder (594 times) and loss of life or personal injury (568 times).
- Information obtained under interception warrants was used in 2,514 arrests, 5,887 prosecutions and 2,460 convictions[1].
- There were 807 stored communications warrants that were issued to 11 criminal law enforcement agencies. This is a decrease of 191 on the 998 issued in 2020-21.
- There was one application for a stored communications warrant that was refused. This was an increase from 2020-21.
- Seven enforcement agencies made 357 arrests, conducted 594 proceedings, and obtained 389 convictions involving evidence obtained under stored communications warrants.
- Twenty enforcement agencies made 310,593 authorisations for the disclosure of existing telecommunications data. This is a decrease of 7,702 authorisations from the 318,295 authorisations made in 2020-21. Of these, 304,652 were made to enforce the criminal law.
- Authorisations for existing telecommunications data covered a range of crimes, including 65,585 authorisations for illicit drug offences, 29,111 authorisations for homicide and 27,506 authorisations for fraud.
- There were 38,097 authorisations were made by 20 criminal law-enforcement agencies for disclosure of prospective telecommunications data. This is a decrease of 1,192 on the 39,289 authorisations made in 2020-21.
- No Journalist Information Warrants were issued to enforcement agencies in 2021-22, consistent with 2020-21.
- There were 30 technical assistance requests given to designated communications providers by four interception agencies. This is an increase of four from 2020-21.
- No technical assistance notices or technical capability notices were given in this reporting period.

[1] The figures provided should be interpreted with some caution as it is only an indication on the effectiveness of interception. For a more detailed interpretation of effectiveness of interception warrants please refer to page 18 of this annual report.

CHAPTER 1 - INTRODUCTION

The 2021–22 Annual Report under the *Telecommunications (Interception and Access) Act 1979* (TIA Act) and Part 15 of the *Telecommunications Act 1997* (Telecommunications Act) sets out the extent and circumstances in which eligible Commonwealth, State and Territory agencies have used the powers available under the TIA Act and Part 15 of the Telecommunications Act between 1 July 2021 and 30 June 2022.

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. Law enforcement agencies' use of warrants and authorisations related to these powers is independently overseen by the Commonwealth Ombudsman (the Ombudsman) and/or equivalent state bodies.

Part 15 of the Telecommunications Act provides a framework for national security and law enforcement agencies to obtain technical assistance from designated communication providers. The industry assistance framework does not replace the need for agencies to obtain a warrant or authorisation to access information. Rather, it facilitates the use of such powers, and provides a formal structure for obtaining assistance.

Access to the content of a communication

Accessing the 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. Except in limited circumstances, such as a life-threatening emergency, interception of communications or access to stored communications can only occur under the authority of a warrant. Such access is subject to significant safeguards, including oversight, record-keeping and reporting obligations. This annual report is an important part of this accountability framework as it provides the public with information about how these powers are used.

Accessing communications is an effective investigative tool that supports and complements information obtained by other methods.

Telecommunications data

Another critical tool available under the TIA Act is access to telecommunications data.[2]

Telecommunications data is often the first source of lead information for investigations, helping to eliminate potential suspects and to consider whether more intrusive investigative tools including search warrants and interception warrants are required. For example, an examination of call charge records can show that an individual may not have had contact with suspects being investigated.

Telecommunications data gives agencies a method for identifying users of a telecommunication service. 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.

Enforcement agencies can access existing telecommunications data[3] and only criminal law-enforcement agencies[4] can access prospective telecommunications data[5] to assist in the investigation of offences punishable by at least three years' imprisonment.

Amendments to the TIA Act in 2015 reduced the number of enforcement agencies that could access telecommunications data under the TIA Act to 21 specified agencies. The Attorney-General may declare additional agencies in limited circumstances for a period of 40 sitting days of Parliament. In the 2021-22 reporting period the NSW Department of Communities and Justice was declared as an enforcement agency.

[2] Telecommunications data is information about a communication (such as the phone number 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) or carriage services supplied (such as information about the identity of the subscriber) – but not the content of the communication.
[3] Existing data, also known as historical data, is information that is already in existence when an authorisation for disclosure is received by a carrier.
[4] 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.
[5] Prospective data is telecommunications data that comes into existence during a period of time in which an authorisation is in force.

CHAPTER 2 – TELECOMMUNICATIONS INTERCEPTION

The interception of communications is regulated by Chapter 2 of the TIA Act. The primary function of Chapter 2 of the TIA Act 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, ACIC, State and Territory police forces and integrity agencies. Only interception agencies are eligible to apply under Part 2-5 of the TIA Act for an interception warrant.

The TIA Act provides for several types of warrants that enable interception of communications passing over a telecommunications system (for example, a phone call between two parties). During the reporting period, interception warrants were available to 17 Commonwealth, State and Territory 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 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.[6]

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

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

This information is presented in **Table 1**. Consistent with previous years, in 2021–22 the majority of warrants obtained were to assist with investigations into serious drug offences and/or trafficking (1,508 warrants). Murder was specified in 594 warrants and 568 related to loss of life or personal injury. 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**.

[6] There are exceptions to this threshold. Interception warrants may be available for offences with a penalty of less than seven years' imprisonment that are of a serious nature, or involve the use of the telecommunications system, such as money laundering. In these circumstances interception of a communication is critical to enable the collection of evidence and its availability may be key to resolving an investigation.

Table 1: Categories of serious offences specified in 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 (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	-	28	12	-	-	-	-	-	-	-	-	-	-	-	-	-	**40**
Assisting person to escape or dispose of proceeds	-	-	4	-	-	-	-	-	-	-	-	4	-	-	-	-	**8**
Bribery, corruption and dishonesty offences	-	46	9	23	10	2	13	3	-	7	2	2	-	-	1	2	**120**
Child abuse offences	-	-	10	-	-	-	-	-	-	1	-	1	-	-	3	-	**15**
Conspire/aid/abet serious offence	-	-	4	-	-	2	-	-	3	16	-	-	-	-	-	-	**25**
Cybercrime offences	-	-	4	-	-	-	-	-	-	-	-	-	-	-	-	-	**4**
Espionage and foreign interference	-	-	9	-	-	-	-	-	-	-	-	-	-	-	-	-	**9**
Kidnapping	-	-	3	-	-	-	-	-	-	57	-	-	6	-	-	2	**68**
Loss of life or personal injury	-	-	20	-	-	-	-	1	-	434	-	35	-	-	36	42	**568**
Money laundering	-	-	77	-	-	-	4	-	16	9	2	-	2	-	-	13	**123**
Murder	-	-	40	-	-	-	-	8	6	434	-	22	5	8	29	42	**594**
Offences involving planning and organisation	-	-	6	-	-	-	-	-	-	90	-	2	-	-	4	56	**158**

Categories of offences	ACIC	ACLEI	AFP	CCC (WA)	IBAC	ICAC (SA)	LECC	NT Police	NSW CC	NSW Police	QLD CCC	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Organised offences and/or criminal organisations	-	-	11	-	-	-	-	-	5	25	-	-	-	-	-	-	**41**
People smuggling and related	-	-	5	-	-	-	-	-	-	-	-	-	-	-	-	-	**5**
Serious damage to property/and/or serious arson	-	-	1	-	-	-	-	1	-	41	-	8	-	-	8	9	**68**
Serious drug offences and/or trafficking	-	12	330	-	-	-	-	22	37	748	16	158	9	4	44	128	**1,508**
Serious fraud	-	-	12	-	-	-	-	-	5	37	-	4	-	-	2	3	**63**
Serious loss of revenue	-	-	2	-	-	-	-	-	-	-	-	-	-	-	-	-	**2**
Special ACC investigations	52	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**52**
Terrorism offences	-	-	65	-	-	-	-	-	-	1	-	-	-	-	-	-	**66**
TOTAL	**52**	**86**	**624**	**23**	**10**	**4**	**17**	**35**	**72**	**1,900**	**20**	**236**	**22**	**12**	**127**	**297**	**3,537**

Eligibility to issue an interception warrant

An interception warrant under Part 2-5 of the TIA Act 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, and
- Federal Circuit and Family Court of Australia.

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).

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

- 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.

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 **Table 2**. As at 30 June 2022, there were 103 issuing authorities for interception warrants.

Table 2: Federal Court judges, Federal Circuit and Family Court judges, and nominated AAT members eligible to issue interception warrants – paragraph 103(ab)

Issuing authority	Number eligible
Federal Court judges	21
Federal Circuit and Family Court judges	46
Nominated AAT members	36
TOTAL	**103**

Issuing of interception warrants

Table 3 states which issuing authorities considered applications for warrants made by each interception agency during 2021-22. In 2021-22, nominated AAT members considered 86 percent of total interception warrant applications made.

Table 3: Interception warrant applications considered by Federal Court judges, Federal Circuit and Family Court judges, and nominated AAT members

Agency	Issuing authority			
	Federal Court judges	Federal Circuit and Family Court judges	Nominated AAT members	TOTAL
ACIC	4	4	44	**52**
ACLEI	-	-	20	**20**
AFP	9	27	439	**475**
CCC (WA)	-	23	-	**23**
IBAC	-	-	10	**10**
ICAC (SA)	-	-	2	**2**
LECC	-	-	17	**17**
NT Police	-	35	-	**35**
NSW CC	-	-	59	**59**
NSW Police	-	49	1,755	**1,804**
QLD CCC	-	17	3	**20**
QLD Police	-	154	82	**236**
SA Police	-	-	22	**22**
TAS Police	-	-	12	**12**
VIC Police	-	-	127	**127**
WA Police	-	136	163	**299**
TOTAL	**13**	**445**	**2,755**	**3,213**

Applications for 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 applications, telephone applications and renewal applications for interception warrants made by agencies during the year.

This information is presented in **Table 4**. In 2021–22, agencies were issued 3,207 interception warrants, being a decrease of 274 from 2020–21, where 3,481 warrants were issued. In 2021-22, 592 renewals of interception warrants were issued. This was a decrease of 160 renewals of interception warrants from the 752 issued in the previous reporting period. There was an increase in the number of telephone applications from 4 to 10 in 2021-22.

Table 4: Applications, telephone applications and renewal applications for interception warrants[7] – paragraphs 100(1)(a)-(c) and 100(2)(a)-(c)

Agency	Relevant statistics	Applications for warrants		Telephone applications for warrants		Renewal applications	
		20/21	21/22	20/21	21/22	20/21	21/22
ACIC	Made	72	52	-	-	23	6
	Refused	-	-	-	-	-	-
	Issued	72	52	-	-	23	6
ACLEI	Made	-	20	-	-	-	7
	Refused	-	-	-	-	-	-
	Issued	-	20	-	-	-	7
AFP	Made	653	475	-	-	199	126
	Refused	-	3	-	-	-	-
	Issued	653	472	-	-	199	126
CCC (WA)	Made	31	23	-	-	12	-
	Refused	-	-	-	-	-	-
	Issued	31	23	-	-	12	-
IBAC	Made	12	10	-	-	5	2
	Refused	2	-	-	-	-	-
	Issued	10	10	-	-	5	2

[7] 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.

Agency	Relevant statistics	Applications for warrants		Telephone applications for warrants		Renewal applications	
		20/21	21/22	20/21	21/22	20/21	21/22
NSW (ICAC)	Made	11	-	-	-	2	-
	Refused	-	-	-	-	-	-
	Issued	11	-	-	-	2	-
ICAC (SA)	Made	10	2	-	-	1	-
	Refused	-	-	-	-	-	-
	Issued	10	2	-	-	1	-
LECC	Made	26	17	-	-	10	5
	Refused	-	-	-	-	-	-
	Issued	26	17	-	-	10	5
NT Police	Made	32	35	-	-	1	5
	Refused	-	-	-	-	-	-
	Issued	32	35	-	-	1	5
NSW CC	Made	97	59	-	-	34	26
	Refused	-	-	-	-	-	-
	Issued	97	59	-	-	34	26
NSW Police	Made	1,755	1,804	2	10	379	326
	Refused	-	1	-	-	-	-
	Issued	1,755	1,803	2	10	379	326
QLD CCC	Made	31	20	-	-	3	10
	Refused	-	-	-	-	-	-
	Issued	31	20	-	-	3	10
QLD Police	Made	249	236	-	-	42	40
	Refused	1	-	-	-	-	-
	Issued	248	236	-	-	42	40

Agency	Relevant statistics	Applications for warrants		Telephone applications for warrants		Renewal applications	
		20/21	21/22	20/21	21/22	20/21	21/22
SA Police	Made	34	22	-	-	2	4
	Refused	-	-	-	-	-	-
	Issued	34	22	-	-	2	4
TAS Police	Made	9	12	-	-	1	1
	Refused	-	-	-	-	-	-
	Issued	9	12	-	-	1	1
VIC Police	Made	139	127	2	-	11	15
	Refused	4	-	-	-	-	-
	Issued	135	127	2	-	11	15
WA Police	Made	327	299	-	-	27	19
	Refused	-	2	-	-	-	-
	Issued	327	297	-	-	27	19
TOTAL	**Made**	**3,488**	**3,213**	**4**	**10**	**752**	**592**
	Refused	**7**	**6**	**-**	**-**	**-**	**-**
	Issued	**3,481**	**3,207**	**4**	**10**	**752**	**592**

Warrants that authorise entry on premises

The TIA Act provides that an issuing authority can issue an interception warrant that authorises entry on premises. An issuing authority can only issue such a warrant if satisfied that it would be impracticable or inappropriate to intercept communications other than by use of equipment installed on those premises.

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 a request to authorise entry on premises.

In 2021–22, an agency was issued one warrant authorising entry on premises. This is an increase from 2020–21, where no such warrants were issued. This information is presented in **Table 5**.

Table 5: Warrants that authorise entry on premises – paragraphs 100(1)(d) and 100(2)(d)

Agency	Applications for warrants	
	20/21	21/22
CCC (WA)	-	1
TOTAL	-	1

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 during the year specified contained conditions or restrictions relating to interceptions under the warrants.

This information is presented in **Table 6**. In 2021-22, 107 interception warrants were issued with a condition or restriction. This is an increase of 43 compared to the 64 issued in 2020–21.

Table 6: Interception warrants issued with specific conditions or restrictions – paragraphs 100(1)(e) and 100(2)(e)

Agency	Telecommunications interception warrants issued specifying conditions or restrictions	
	20/21	21/22
ACLEI	-	2
AFP	1	1
LECC	4	2
NT Police	2	-
NSW CC	1	-
NSW Police	56	99
QLD CCC	-	3
TOTAL	**64**	**107**

Effectiveness of 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 separately report on the number of times lawfully intercepted information derived from their warrants culminated in an arrest by another agency. This removes the risk that arrest numbers will be duplicated due to multiple agencies reporting on the same arrest. This also shows the outcomes from agencies that do not have arrest powers themselves but where lawfully intercepted information derived from their warrants, ultimately leads to an arrest by another agency.

Paragraphs 102(1)(b)-(c) and 102(2)(b)-(c) of the TIA Act 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.

This information is provided in **Tables 7, 8 and 9**. In 2021–22, there were 2,514 arrests made as a result of lawfully intercepted information. There were also 5,887 prosecutions and 2,460 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 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 result in prosecution or conviction for a number of offences, some or all of which may occur at a later time.

The statistics may also understate the effectiveness of interception, as prosecutions may be initiated or convictions entered 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 7: Arrests on the basis of lawfully intercepted information – paragraphs 102(1)(a) and 102(2)(a)

Agency	20/21		21/22	
	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	-	27	-	20
ACLEI	-	-	2	2
AFP	132	44	125	7
ICAC (SA)	-	1	2	1
LECC	-	1	-	-
NT Police	25	14	22	-
NSW CC	-	107	-	57
NSW Police	1,478	13	1,471	7
QLD CCC	20	14	-	3
QLD Police	316	-	227	-
SA Police	53	-	27	-
TAS Police	17	-	3	3
VIC Police	269	42	325	48
WA Police	407	347	310	218
TOTAL	**2,717**	**610**	**2,514**	**366**

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

Category	ACLEI	ACIC	AFP	IBAC	ICAC (SA)	NT Police	NSW CC	NSW Police	QLD CCC	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Administration of justice / government offence	-	-	2	-	-	-	-	-	-	-	-	-	-	-	**2**
Ancillary offences	-	-	3	-	-	-	-	-	-	-	-	-	8	-	**11**
Assisting person to escape or dispose of proceeds	-	-	-	-	-	-	-	-	-	-	-	-	1	-	**1**
Bribery or corruption	2	-	-	6	1	-	-	-	-	-	-	-	2	4	**15**
Child abuse offences	-	-	1	-	-	-	-	1	-	-	-	-	-	7	**9**
Conspire/aid/abet serious offence	-	-	-	-	-	-	-	14	3	-	-	-	2	-	**19**
Cybercrime offences	-	-	3	-	-	-	-	-	-	-	-	-	-	-	**3**
Espionage foreign interference	-	-	2	-	-	-	-	-	-	-	-	-	-	-	**2**
Kidnapping	-	-	-	-	-	-	1	60	-	-	-	-	-	-	**61**
Loss of life	-	-	-	-	-	-	-	18	-	-	-	-	2	5	**25**
Money laundering	-	-	16	-	1	-	-	24	1	-	-	-	8	37	**87**
Murder	-	-	-	-	-	-	-	68	-	1	1	1	4	9	**84**
Offences involving planning and organisation	-	-	1	-	-	-	-	121	-	-	-	-	28	85	**235**
Organised crime	-	-	-	-	-	-	-	86	-	-	-	-	-	-	**86**

Category	ACLEI	ACIC	AFP	IBAC	ICAC (SA)	NT Police	NSW CC	NSW Police	QLD CCC	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Other offences punishable by 3 years to life	-	-	22	-	-	-	-	27	-	39	-	-	51	-	**139**
Serious arson	-	-	-	-	-	-	-	19	-	-	-	-	3	5	**27**
Serious damage to property	-	-	-	-	-	-	-	13	-	-	-	-	-	8	**21**
Serious drug offences and/or trafficking	-	1	65	-	2	22	2	3,130	5	38	-	3	74	1,126	**4,468**
Serious fraud	-	-	-	-	-	-	-	14	3	-	-	-	-	6	**23**
Serious loss of revenue	-	-	1	-	-	-	-	-	-	-	-	-	-	-	**1**
Serious personal injury	-	-	-	-	-	-	-	507	-	-	2	-	30	18	**557**
Telecommunications offences	-	-	6	-	-	-	-	-	-	-	-	-	-	-	**6**
Terrorism offences	-	-	5	-	-	-	-	-	-	-	-	-	-	-	**5**
TOTAL	**2**	**1**	**127**	**6**	**4**	**22**	**3**	**4,102**	**12**	**78**	**3**	**4**	**213**	**1,310**	**5,887**

Table 9: 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	AFP	IBAC	NSW CC	NSW Police	QLD CCC	QLD Police	SA Police	VIC Police	WA Police	TOTAL
Administration of justice / government offence	-	1	-	-	-	-	-	-	-	-	**1**
Ancillary Offences	-	2	-	-	-	-	-	-	8	-	**10**
Assisting person to escape or dispose of proceeds	-	-	-	-	-	-	-	-	1	-	**1**
Bribery or corruption	-	-	3	-	-	-	-	-	-	2	**5**
Child abuse offences	-	3	-	-	-	-	-	-	-	4	**7**
Conspire/aid/abet serious offence	-	-	-	-	4	1	-	-	2	-	**7**
Kidnapping	-	-	-	-	29	-	-	-	-	-	**29**
Loss of life	-	-	-	-	14	-	-	-	2	2	**18**
Money laundering	-	12	-	-	3	1	-	-	8	19	**43**
Murder	-	-	-	-	29	-	1	1	-	4	**35**
Offences involving planning and organisation	-	7	-	-	87	-	-	-	28	52	**174**
Organised crime	-	-	-	-	28	-	-	-	-	-	**28**

Category	ACIC	AFP	IBAC	NSW CC	NSW Police	QLD CCC	QLD Police	SA Police	VIC Police	WA Police	TOTAL
Other offences punishable by 3 years to life	-	10	-	-	14	-	39	-	51	-	**114**
Serious arson	-	-	-	-	5	-	-	-	3	3	**11**
Serious damage to property	-	-	-	-	-	-	-	-	-	3	**3**
Serious drug offences and/or trafficking	1	54	-	1	715	5	38	-	72	780	**1,666**
Serious fraud	-	-	-	-	61	3	-	-	-	3	**67**
Serious loss of revenue	-	1	-	-	-	-	-	-	-	-	**1**
Serious personal injury	-	-	-	-	184	-	-	-	27	11	**222**
Telecommunications offences	-	8	-	-	-	-	-	-	-	-	**8**
Terrorism offences	-	10	-	-	-	-	-	-	-	-	**10**
TOTAL	**1**	**108**	**3**	**1**	**1,173**	**10**	**78**	**1**	**202**	**883**	**2,460**

Named person warrants

A named person warrant can authorise the interception of multiple telecommunications services (such as a landline or mobile service), or 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 a number of matters including:

- how much the privacy of any person would be likely to be interfered with
- the gravity of the conduct constituting the offence
- the extent to which the interception would be likely to 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) of the TIA Act provide that this report must set out the relevant statistics about applications, telephone applications and renewal applications for named person warrants, and how many named person warrants issued on applications made by an agency during the year specified conditions or restrictions relating to interceptions under the warrants.

This information is presented in **Tables 10 and 11**. In 2021–22, 458 named person warrants were issued. This is a decrease of 75 from 2020–21, in which 533 named person warrants were issued. There was also a decrease of 29 renewal applications from 151 in 2020-21 to 122 in 2021-22.

Table 10: Applications, telephone applications, and renewal applications for named person warrants – paragraphs 100(1)(ea) and 100(2)(ea)[8]

Agency	Relevant Statistics	Applications for named person warrants		Telephone applications for named person warrants		Renewal applications for named person warrants	
		20/21	21/22	20/21	21/22	20/21	21/22
ACIC	Made	39	23	-	-	13	2
	Refused	-	-	-	-	-	-
	Issued	39	23	-	-	13	2
AFP	Made	196	149	-	-	63	42
	Refused	-	-	-	-	-	-
	Issued	196	149	-	-	63	42
CCC (WA)	Made	3	4	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	3	4	-	-	-	-
IBAC	Made	6	2	-	-	3	-
	Refused	-	-	-	-	-	-

[8] 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	
		20/21	21/22	20/21	21/22	20/21	21/22
	Issued	6	2	-	-	3	-
LECC	Made	6	13	-	-	5	5
	Refused	-	-	-	-	-	-
	Issued	6	13	-	-	5	5
NT Police	Made	1	5	-	-	-	2
	Refused	-	-	-	-	-	-
	Issued	1	5	-	-	-	2
NSW CC	Made	46	26	-	-	13	17
	Refused	-	-	-	-	-	-
	Issued	46	26	-	-	13	17
NSW Police	Made	93	133	-	1	34	37
	Refused	-	-	-	-	-	-
	Issued	93	133	-	1	34	37
QLD CCC	Made	3	5	-	-	2	2
	Refused	-	-	-	-	-	-
	Issued	3	5	-	-	2	2
QLD Police	Made	31	28	-	-	5	7
	Refused	-	-	-	-	-	-
	Issued	31	28	-	-	5	7
SA Police	Made	4	7	-	-	-	2
	Refused	-	-	-	-	-	-
	Issued	4	7	-	-	-	2
TAS Police	Made	2	-	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	2	-	-	-	-	-
VIC Police	Made	35	22	-	-	4	4
	Refused	1	-	-	-	-	-
	Issued	34	22	-	-	4	4
WA Police	Made	69	41	-	-	9	2
	Refused	-	-	-	-	-	-
	Issued	69	41	-	-	9	2
TOTAL	**Made**	**534**	**458**	**0**	**1**	**151**	**122**
	Refused / Withdrawn	**1**	**0**	**0**	**0**	**0**	**0**
	Issued	**533**	**458**	**0**	**1**	**151**	**122**

In 2021–22, 5 named person warrants were issued with a condition or restriction. This is a decrease of 6 compared to the 11 issued with a condition or restriction in 2020-21.

Table 11: Named person warrants issued with specific conditions or restrictions – paragraphs 100(1)(ea) and 100(2)(ea)

Agency	Named person warrants issued specifying conditions or restrictions	
	20/21	21/22
AFP	1	-
LECC	4	2
NSW CC	1	-
NSW Police	2	2
QLD CCC	3	1
TOTAL	**11**	**5**

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 the table below. This information is outlined in **Table 12**. Consistent with previous reporting periods, in 2021–22 the majority of named person warrants related to 2 to 5 telecommunications services.

Table 12: Named person warrants by reference to services intercepted under the warrant – paragraphs 100(1)(eb) and 100(2)(eb)

Agency	Named person warrants by number of services intercepted							
	1 service only		2 – 5 services		6 – 10 services		10+ services	
	20/21	21/22	20/21	21/22	20/21	21/22	20/21	21/22
ACIC	12	11	26	10	1	-	-	-
AFP	85	34	97	94	6	7	5	-
CCC (WA)	2	3	1	1	-	-	-	-
IBAC	-	-	6	2	-	-	-	-
LECC	1	-	4	13	1	-	-	-
NT Police	-	-	1	5	-	-	-	-
NSW CC	20	7	26	19	-	-	-	-
NSW Police	32	51	58	78	3	6	-	-
QLD CCC	-	2	-	2	3	1	-	-
QLD Police	8	10	20	14	3	4	-	-
SA Police	1	1	3	6	-	-	-	-
TAS Police	-	-	1	-	1	-	-	-
VIC Police	14	6	20	15	-	1	-	-
WA Police	22	7	45	30	2	4	-	-
TOTAL	**197**	**132**	**308**	**289**	**20**	**23**	**5**	**-**

Under the TIA Act, agencies can apply for a named person warrant in relation to telecommunications devices.

Subparagraphs 100(1)(ec)(i)-(iii) and 100(2)(ec)(i)-(iii) require the report to include the total number of:

i. services[9] intercepted under service based named person warrants

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

iii. telecommunications devices[10] intercepted under device-based named person warrants.

The number of services and devices intercepted under the different types of named person warrants are outlined in **Tables 13 and 14**.

Table 13: Total number of services intercepted under service-based named person warrants – paragraphs 100(1)(ec) and 100(2)(ec)

Agency	Services	
	20/21	21/22
ACIC	60	36
AFP	427	335
CCC WA	4	4
IBAC	20	5
LECC	18	35
NT Police	1	15
NSW CC	46	26
NSW Police	205	138
QLD CCC	6	12
QLD Police	77	81
SA Police	7	16
TAS Police	9	-
VIC Police	67	52
WA Police	141	106
TOTAL	**1,088**	**861**

[9] A telecommunications service is defined at section 5 of the TIA Act and means a service for carrying communications by means of guided or unguided electromagnetic energy or both, being a service the use of which enables communications to be carried over a telecommunications system operated by a carrier but not being a service for carrying communications solely by means of radiocommunications.

[10] A telecommunications device is defined at section 5 of the TIA Act and means a terminal device that is capable of being used for transmitting or receiving communication over a telecommunications system.

Table 14: Total number of services and devices intercepted under device-based named person warrants – paragraphs 100(1)(ec) and 100(2)(ec)

Agency	Devices		Services	
	20/21	21/22	20/21	21/22
ACIC	24	-	26	-
AFP	94	21	51	30
NT Police	-	2	-	-
NSW Police	14	18	38	39
WA Police	6	2	-	-
TOTAL	**138**	**43**	**115**	**69**

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 the agency has exhausted all other practicable methods of identifying the telecommunications services used by 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) of the TIA Act provide that this report must set out the relevant statistics about applications, telephone applications and renewal applications for B-Party warrants. This report must also set out how many B-Party warrants were issued and the number of applications made by an agency during the year, including requests to authorise entry on premises, and specified conditions or restrictions relating to interception under the warrants.

This information is presented in **Tables 15 and 16**. In 2021–22, 57 B-Party warrants were issued to interception agencies. This represents an increase of three from the 54 B-Party warrants issued in 2020–21.

Table 15: Applications for B-Party warrants, telephone applications and renewal applications for B-Party warrants – paragraphs 100(1)(ed) and 100(2)(ed)[11]

Agency	Relevant statistics	Applications for B-Party warrants		Telephone applications for B-Party warrants		Renewal applications for B-Party warrants	
		20/21	21/22	20/21	21/22	20/21	21/22
ACIC	Made	1	2	-	-	-	1
	Refused	-	-	-	-	-	-
	Issued	1	2	-	-	-	1
AFP	Made	17	11	-	-	10	3
	Refused	-	1	-	-	-	-
	Issued	17	10	-	-	10	3
NSW Police	Made	36	43	2	2	-	2
	Refused	-	-	-	-	-	-
	Issued	36	43	2	2	-	2
QLD Police	Made	-	1	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	-	1	-	-	-	-
VIC Police	Made	1	1	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	1	1	-	-	-	-
TOTAL	**Made**	**54**	**58**	**2**	**2**	**10**	**6**
	Refused	**0**	**1**	**0**	**-**	**0**	**-**
	Issued	**54**	**57**	**2**	**2**	**10**	**6**

In 2021–22, four B-Party warrants were issued with conditions or restrictions. This is an increase of one from the three issued in 2020–21.

Table 16: B-Party warrants issued with conditions or restrictions – Paragraphs 100(1)(ed) and 100(2)(ed)

Agency	B-party warrants specifying conditions or restrictions	
	20/21	21/22
AFP	-	1
NSW Police	3	3
TOTAL	**3**	**4**

In 2021-22, no B-Party warrants were issued on applications made by an agency authorised entry onto premises. This is the same as the previous year.

[11] 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.

Duration of warrants

Under the TIA Act, an interception warrant, other than a B-Party warrant, can be in force for up to 90 days. Under section 57, the chief officer of an agency may revoke a warrant at any time and must revoke a warrant if they are satisfied that the grounds on which the warrant was issued 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 17: Duration of original and renewal 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)[12]	Average period specified in warrants (days)	Average period warrants in force (days)[13]
ACLEI	76	60	90	66
ACIC	90	72	90	76
AFP	84	65	86	72
CCC (WA)	90	53	-	-
IBAC	75	53	90	90
ICAC (SA)	57	17	-	-
LECC	90	81	90	40
NT Police	90	77	90	90
NSW CC	83	68	84	73
NSW Police	74	50	78	61
QLD CCC	80	78	79	79
QLD Police	78	59	69	59
SA Police	81	69	90	88
TAS Police	67	56	90	61
VIC Police	87	56	71	50
WA Police	84	42	88	66
AVERAGE	**78**	**53**	**80**	**65**

A B-Party warrant can be in force for up to 45 days. Paragraphs 101(1)(da) and 101(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.

[12] This column excludes warrants that did not cease before the end of the reporting period.
[13] This column excludes warrants that did not cease before the end of the reporting period.

Table 18: 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	45	36
AFP	40	38	45	40
NSW Police	32	18	40	27
QLD Police	29	20	-	-
VIC Police	45	40	-	-
AVERAGE	**34**	**23**	**43**	**35**

Final renewals

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

Information on the number of final renewals of warrants by agencies is presented in **Table 19.**

Table 19: Final renewals – paragraphs 101(1)(e) and 101(2)(e)

Agency	91-150 days		151-180 days		> 180 days	
	20/21	21/22	20/21	21/22	20/21	21/22
ACIC	10	4	-	-	3	-
ACLEI	-	-	-	-	-	3
AFP	5	26	39	28	46	34
CCC (WA)	9	-	3	-	-	-
IBAC	4	-	3	2	-	-
ICAC (NSW)	2	-	-	-	-	-
LECC	-	2	7	1	1	-
NT Police	-	-	-	-	-	1
NSW CC	4	2	4	1	5	6
NSW Police	122	118	36	53	63	64
QLD CCC	-	4	-	-	-	-
QLD Police	23	9	11	7	1	8
SA Police	4	2	-	-	-	1
VIC Police	8	4	3	6	-	1
WA Police	13	15	18	4	-	1
TOTAL	**204**	**186**	**124**	**102**	**119**	**119**

Eligible warrants

Definition

An **'eligible warrant'** is a warrant that was in force during the reporting period – not necessarily a warrant that was issued during the reporting period – where a prosecution was instituted or was likely to be instituted on the basis of information obtained by interceptions under the warrant.

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

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.

This information is presented in **Table 20**. In 2021–22, 64 per cent of total warrants were eligible warrants.

Table 20: Percentage of eligible warrants – paragraphs 102(3) and 102(4)[14]

Agency	Number of eligible warrants	Total number of warrants in force	%
ACIC	18	62	29%
ACLEI	20	20	100%
AFP	100	550	18%
CCC (WA)	1	24	4%
IBAC	8	10	80%
ICAC (SA)	3	5	60%
LECC	2	17	12%
NT Police	7	35	20%
NSW CC	44	72	61%
NSW Police	1577	2046	77%
QLD CCC	8	20	40%
QLD Police	254	269	94%
SA Police	26	31	84%
TAS Police	4	11	36%
VIC Police	101	150	67%
WA Police	147	326	45%
TOTAL	**2,320**	**3,648**	**64%**

[14] Total number of warrants in force is often larger than the number of warrants issued as it includes warrants issued in the previous reporting period but still in force during the current reporting period.

Interception without a warrant

Under subsections 7(4) and 7(5) of the TIA Act, an agency can undertake interception without a warrant in the event of an emergency. 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 7(5).

In 2021–22, there were no instances where agencies intercepted communications under subsections 7(4) or 7(5) of the TIA Act without a warrant. There was no change from 2020-21.

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

In 2021–22, there were no occasions in which lawfully intercepted information or interception warrant information was provided to a foreign country under international assistance. There was no change from 2020-21.

Number of interceptions carried out on behalf of other agencies

The TIA Act supports the ability of interception agencies to cooperate and work collaboratively by enabling one interception agency to carry out interception on behalf of other interception 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 21: 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**	11
AFP	**ACIC**	13
AFP	**ACLEI**	20

Interception carried out by:	Interception carried out on behalf of:	Number of interceptions
CCC (WA)	ICAC (SA)	2
CCC (WA)	WA Police	22
VIC Police	QLD CCC	17
VIC Police	TAS Police	12
TOTAL		97

Telecommunications interception expenditure

Table 22 provides information about the total expenditure (including expenditure of a capital nature) incurred by interception agencies in connection with interception warrants and the average expenditure 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 22: Total expenditure incurred by each agency in connection with the execution of interception warrants and average expenditure per interception warrant – paragraphs 103(a) and 103(aa)

Agency	Total expenditure	Average expenditure
ACIC	$5,064,833	$97,401
ACLEI	$225,377	$11,269
AFP	$12,425,044	$26,324
CCC (WA)	$551,883	$23,995
IBAC	$755,052	$75,505
ICAC (NSW)	$429,113	-
ICAC (SA)	$76,351	$38,176
LECC	$733,745	$43,161
NT Police	$1,219,673	$34,848
NSW CC	$1,631,163	$27,647
NSW Police	$10,051,821	$5,575
QLD CCC	$1,696,337	$84,817
QLD Police	$6,000,344	$25,425
SA Police	$4,228,924	$192,224
TAS Police	$870,163	$72,514
VIC Police	$549,529	$4,327
WA Police	$3,940,175	$13,267
TOTAL / AVERAGE	**$50,449,527**	**$15,731**

The breakdown of the total recurrent costs of interception over the reporting period is provided in **Table 23**. 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 23: Recurrent interception costs per agency

Agency	Salaries	Administrative Support	Capital expenditure	Interception costs	Total ($)
ACIC	$3,596,927	$412,006	-	$1,055,900	**$5,064,833**
ACLEI	$220,277	-	-	$5,100	**$225,377**
AFP	$7,984,829	$248,695	-	$4,191,519	**$12,425,044**
CCC (WA)	$264,489	$450	$220,688	$66,256	**$551,883**
IBAC	$565,152	$24,340	$62,787	$102,773	**$755,052**
ICAC (NSW)	$233,715	-	-	$195,398	**$429,113**
ICAC (SA)	$4,896	$71,055	-	$400	**$76,351**
LECC	$694,434	$1,908	$7,117	$30,286	**$733,745**
NT Police	$923,945	$192,341	$91,759	$11,628	**$1,219,673**
NSW CC	$1,218,730	$619	-	$411,814	**$1,631,163**
NSW Police	$7,309,442	$361,143	-	$2,381,236	**$10,051,821**
QLD CCC	$1,193,012	$269,249	-	$234,076	**$1,696,337**
QLD Police	$4,626,191	$681,138	$411,046	$281,969	**$6,000,344**
SA Police	$2,643,696	$161,268	$549,339	$874,621	**$4,228,924**
TAS Police	$773,394	$9,393	$6,702	$80,674	**$870,163**
VIC Police	$486,773	$5,497	$18,486	$38,773	**$549,529**
WA Police	$3,423,430	$171,627	-	$345,118	**$3,940,175**
TOTAL	**$36,163,332**	**$2,610,729**	**$1,367,924**	**$10,307,541**	**$50,449,527**

Emergency service facilities

Under the TIA Act, listening to or recording calls to and from a facility declared by the Attorney-General to be an emergency service facility does not constitute interception. This exemption ensures that emergency service providers 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 24** sets out the number of premises that have been declared in 2020-21 under the TIA Act to be emergency service facilities.

Table 24: Emergency service facility declaration – paragraph 103(ad)

Agency	Police	Fire brigade	Ambulance	Despatching
Australian Capital Territory	-	-	-	1
TOTAL	**0**	**0**	**0**	**1**

Safeguards and reporting requirements on interception powers

The TIA Act contains a number of safeguards, controls, and reporting requirements in relation to interception warrants. These include a requirement for:

- the heads of interception agencies to provide the Secretary of AGD with a copy of each interception warrant
- interception agencies to report to the Attorney-General, within three months of a warrant ceasing to be in force, detailing the use of information obtained by interception under the warrant
- the Secretary of AGD to maintain a General Register detailing the particulars of all interception warrants. The Secretary of AGD must provide the General Register to the Attorney-General for inspection every three months, and
- the Secretary of AGD to maintain a Special Register recording the details of interception warrants that do not lead to a prosecution within three months of the warrant expiring. The Special Register is also given to the Attorney-General to inspect.

Interception agencies' use of interception powers under the TIA Act is independently overseen by the Ombudsman and equivalent state oversight and integrity bodies.

At least twice a year the Ombudsman must inspect the records kept by the ACIC, the ACLEI, and the AFP relating to interception, 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 2021.

The Ombudsman is required under the TIA Act to report to the Attorney-General about these inspections, including information about any deficiencies identified and remedial action. State and Territory legislation imposes similar requirements on State and Territory interception agencies regarding their use of interception powers.

While the 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 Attorney-General. The 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.

Ombudsman – inspection of telecommunications interception records conducted in 2021-22

Overview

During 2021-22, the Ombudsman conducted 5 inspections under subsection 83(1) of the TIA Act. These inspections examined agencies' use of telecommunications interception powers under Chapter 2 of the TIA Act between 1 January and 31 December 2021, and consisted of:

- two inspections at the AFP
- two inspections at the ACIC, and
- one inspection at ACLEI.[15]

The Ombudsman is required to assess agencies' compliance with the record keeping and destruction provisions under sections 79, 79AA, 80 and 81 of the TIA Act. In accordance with section 85 of the TIA Act, the Ombudsman may also report on any other contravention of the TIA Act.

Based on the inspections the Ombudsman was satisfied agencies continued to be generally compliant with the TIA Act and responsive to the Ombudsman's inspection findings. Agencies demonstrated a good understanding of the requirements of the TIA Act and appropriately disclosed non-compliance issues to the Ombudsman.

Below is a summary of the findings from the 5 inspections the Ombudsman conducted during 2021–22. Where agencies advised of action taken to address the Ombudsman's findings, the Ombudsman will review this action during their 2022–23 inspections.

Sections 79 and 79AA: Destruction of restricted records

Sections 79 and 79AA of the TIA Act set out the requirements for destroying restricted records.[16]

Section 79AA of the TIA Act requires the chief officer of an agency to cause destruction of restricted records obtained under a control order warrant in certain circumstances. The Ombudsman did not make any findings in relation to compliance with section 79AA of the TIA Act from inspections conducted during 2021–22.

Subsection 79(1) of the TIA Act provides that, where the chief officer of an agency is satisfied a restricted record is not likely to be required for a permitted purpose, the chief officer must cause the restricted record to be destroyed forthwith. Under subsection 79(2) of the TIA Act, agencies cannot destroy a restricted record until written notice is received from the Secretary of AGD that the relevant entry in the General Register of interception warrants has been inspected by the Attorney-General.

The TIA Act does not create a requirement for agencies to periodically review restricted records for destruction. However, to demonstrate compliance and noting the high level of privacy intrusion associated with intercepted information, agencies should have a

[15] This inspection considered ACLEI's use of telecommunications interceptions powers between 1 July and 31 December 2021. ACLEI advised it did not use the powers between 1 January and 30 June 2021 which meant the Ombudsman did not need to conduct an inspection for that period.

[16] A restricted record means a record, other than a copy, of a communication passing over a telecommunications system that was obtained by means of an interception, whether or not in contravention of the general prohibition on intercepting communications under subsection 7(1) of the TIA Act. It does not include a record of interception occurring under a warrant issued under the *Surveillance Devices Act 2004*.

process to consider whether restricted records are likely to be required for a permitted purpose and, if not, destroy the records in line with subsection 79(1) of the TIA Act.

ACIC

In 2020–21, the Ombudsman reported the ACIC did not regularly consider when restricted records should be destroyed and had not set an internal timeframe for when destructions are considered completed 'forthwith'. The ACIC advised that it intended to undertake a destructions project which would result in standard procedures and timeframes for ongoing management of restricted record destructions.

During the Ombudsman's 2021–2022 inspections, it found the ACIC had commenced a destructions project. This involved auditing records for review, establishing standardised destruction procedures, and hiring additional staff. However, no destructions were completed in 2021, and the Ombudsman was unable to review any of the ACIC's new processes in action. The Ombudsman will continue monitoring the destructions project.

ACLEI

The Ombudsman identified that ACLEI held restricted records associated with several historical operations which were unlikely to be required for a permitted purpose and had not been subject to the chief officer's consideration for destruction. The Ombudsman suggested ACLEI review these records to ascertain whether associated it was still required for a permitted purpose, and if appropriate, initiate the process of seeking chief officer consideration to authorise their destruction.

AFP

The Ombudsman did not make any destruction related findings for the AFP under section 79 of the TIA Act.

Section 80: Record keeping in connection with telecommunications interception warrants

Section 80 of the TIA Act requires the chief officer of an agency to keep certain documents connected with issuing telecommunications interception warrants. The Ombudsman considers an agency's compliance with record keeping requirements is fundamental to demonstrating accountability for its use of covert and intrusive powers.

Based on inspections the Ombudsman was satisfied that ACLEI, the ACIC and the AFP were compliant with section 80 of the TIA Act.

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, and to record particulars relating to restricted records and lawfully intercepted information.

The Ombudsman assessed that ACLEI, the ACIC and the AFP were compliant with section 81 of the TIA Act. The Ombudsman made one suggestion to the ACIC regarding amending its internal training to clarify that the obligation to keep records of use and communication of lawfully intercepted information extends beyond the life of a warrant.

The AFP advised during the February 2022 inspection that due to the structure of joint task forces, the AFP considered sharing lawfully intercepted information with joint task

force members to be an internal communication. However, the Ombudsman identified 4 instances where the AFP's use and communication of lawfully intercepted information to joint task forces was recorded as external communication. Despite the inconsistencies, the Ombudsman acknowledged that overall, the AFP captured and reported all relevant information as required.

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

Under section 85 of the TIA Act, the Ombudsman may report on other contraventions of the TIA Act.

Assessments include checking whether interceptions were conducted in accordance with warrants, whether the agency properly dealt with any intercepted information and whether agencies complied with any corresponding obligations on interception under Chapter 2 of the TIA Act. The Ombudsman identified the following key issues.

Certified copies of warrant not provided as soon as practicable

Under subsection 60(1) of the TIA Act, where a telecommunications interception warrant is issued to an agency and it is proposed to intercept communications under the warrant, the agency must inform the relevant carrier immediately of the issue of the warrant and provide a certified copy of the warrant as soon as practicable.

The ACIC disclosed several instances where there were delays in providing certified copies of warrants to carriers. The ACIC advised this was to COVID-19 lockdowns.

The Ombudsman reviewed the time periods between the date of issue and the date the certified copy of the warrant was provided to the carrier for the instances disclosed. These periods ranged from 3 to 10 months. The Ombudsman asked the ACIC to provide further information about how the COVID-19 lockdowns had contributed to these significant delays.

The ACIC advised that it was conducting an internal audit on this matter. The ACIC provided reasons for the delays, including that numerous lockdowns in several states made it impossible for investigators to attend offices to forward the original documents to the ACIC Sydney Office, as well as the ACIC Sydney Office experiencing significant lockdowns itself. The Ombudsman will continue to monitor this issue.

Named Person Warrant – devices not in the prescribed form

Subsection 49(1) of the TIA Act requires a telecommunications interception warrant to be in the prescribed form. The prescribed form for a Named Person Warrant – Devices is provided in Form 4 of Schedule 1 of the *Telecommunications (Interception and Access) Regulations 2017* (the Regulations). The prescribed form for a Named Person Warrant – Services is provided in Form 3 of Schedule 1 of the Regulations.

The ACIC disclosed 3 instances where the drafting officer used the Named Person Warrant – Services template, instead of the Named Person Warrant – Devices template. This resulted in known telecommunication devices not being specified on the warrant and the warrants not being in the prescribed form. This issue was identified by ACIC while preparing the section 94 reports to the Attorney-General.

The ACIC quarantined information obtained under these warrants.

During the inspection, the Ombudsman sought to confirm whether the intercepted information had been used or communicated. The ACIC advised that certain information was communicated to the relevant issuing authorities as part of an application to renew the warrants and, as such, the information derived from the subsequent warrants had also been quarantined. The Ombudsman will review this matter again at the next inspection.

Omission of a matter that the issuing authority must be satisfied of

Subsection 46A(3) of the TIA Act provides that an eligible judge or nominated AAT member must not issue a warrant that authorises interception of communications made by means of a telecommunications device or telecommunications devices identified in the warrant unless satisfied that:

> (a) there are no other practicable methods available to the agency at the time of making the application to identify the telecommunications services used, or likely to be used, by the person in response of whom the warrant would be issued; **or**
>
> (b) interception of communications made to or from a telecommunications service used, or likely to be used, by that person would not otherwise be practicable.

This requirement is reflected in paragraph 1(3) of Form 4 in the Regulations.

The Ombudsman identified 2 instances at the ACIC where paragraph 1(3) of Form 4 had been omitted from the warrant.

The Ombudsman advised the ACIC that the 2 warrants did not comply with the prescribed form and do not demonstrate that the issuing authority was satisfied of the matter set out in subsection 46A(3) of the TIA Act. The Ombudsman suggested the ACIC seek legal advice regarding the validity of these warrants, and then appropriately manage intercepted information including through quarantining and confirming use and communication of that information if required.

The ACIC has since advised that it quarantined the information obtained under the 2 affected warrants. The ACIC confirmed this information was not used or disclosed. The ACIC also identified that a renewal of one of the warrants was affected by the same issue. The ACIC revoked the renewal warrant prior to any interception taking place.

Communication of lawfully intercepted information without a section 68 authorisation

During a previous inspection, there were 2 instances where the AFP communicated lawfully intercepted information to another agency, but where in the Ombudsman's view the communication was not made by either the chief officer or an officer authorised by the chief officer. In the Ombudsman's last report to the AFP, the Ombudsman noted the AFP was confirming its position in relation to these 2 instances.

The Ombudsman considered further information provided by the AFP and remains concerned that the investigator released lawfully intercepted information to the external agency without authorisation under s 68 of the TIA Act. The Ombudsman is continuing to engage with the AFP on this matter.

Legal basis for use and communication of lawfully intercepted information and interception warrant information

The Ombudsman found 2 instances where ACLEI shared lawfully intercepted information with AFP to request a welfare check on a non-target third party who was not directly relevant to the investigation.

It was unclear to the Ombudsman how these instances fell under a 'permitted purpose' under section 67 of the TIA Act, and the interaction of this provision with separate provisions of the *Law Enforcement Integrity Commissioner Act 2006* (Cth) regarding confidentiality requirements and exceptions.

It was also unclear whether ACLEI's sharing of lawfully intercepted information with AFP in the context of a joint investigation, should be classified as being sharing for internal use or external communication. The Ombudsman suggested ACLEI further consider these questions and seek legal advice on the appropriate classification of sharing lawfully intercepted information with the AFP. The Ombudsman will continue to engage with ACLEI on these matters.

Other administrative issues

The Ombudsman also reported on administrative issues, including instances where the consequences may be negligible. They identified, and agencies disclosed, several administrative issues involving:

- minor inconsistencies in the AFP control order template form with Form 2A of the TIA Act Regulations
- issues surrounding AFP's Use and Communication logs. There were three instances where the information in the 'Use Made of Information' form was too broad
- AFP inconsistent reporting of use and communication of lawfully intercepted information
- errors in the ACIC's report to the Attorney-General under section 94 of the TIA Act
- ACIC omitting non-applicable paragraphs of the prescribed form, and
- ACLEI lawfully intercepted information subject to Legal Professional Privilege labelled as 'potentially privileged' but not quarantined.

Figure 1: Ombudsman's Telecommunications Interception Inspection Criteria

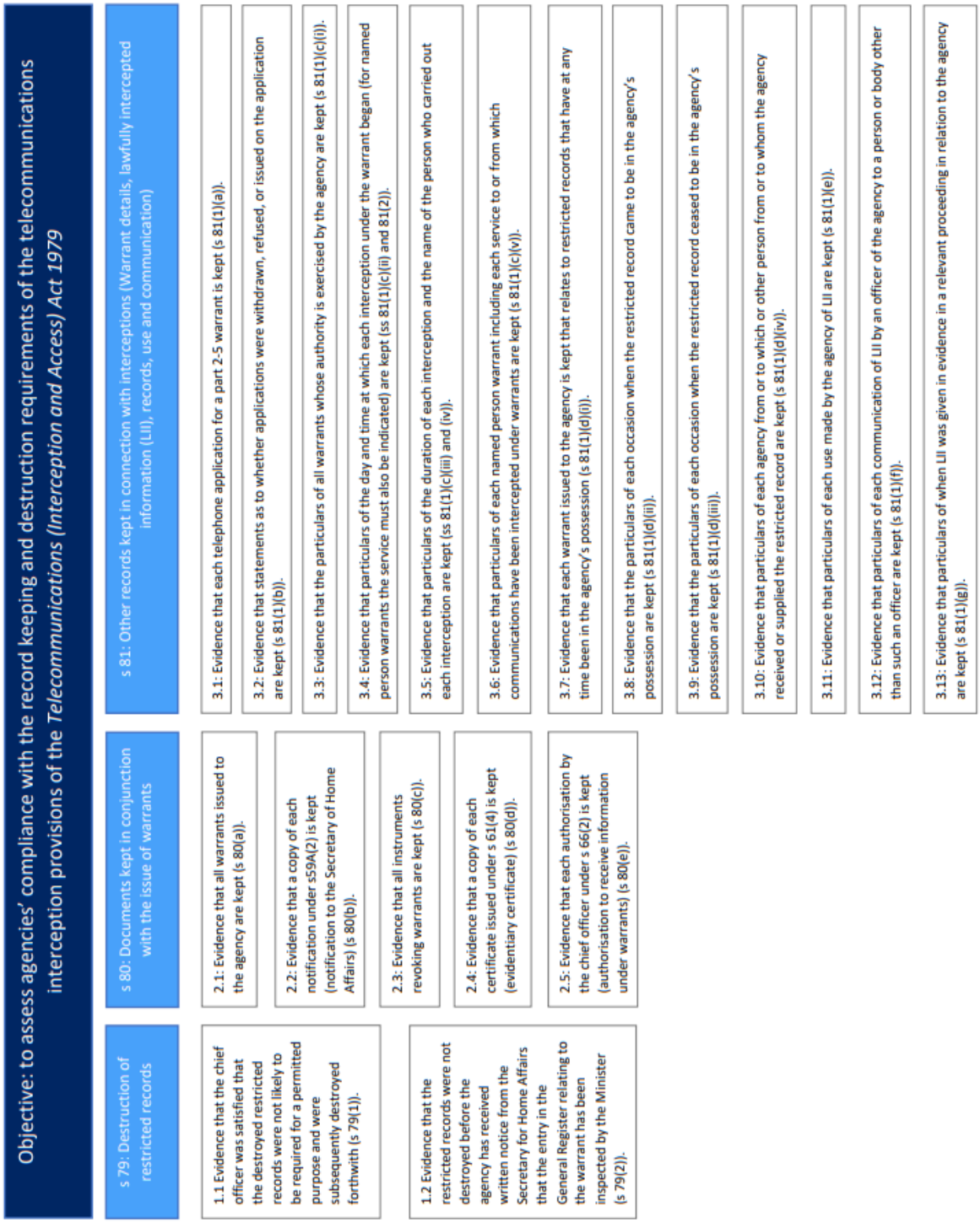
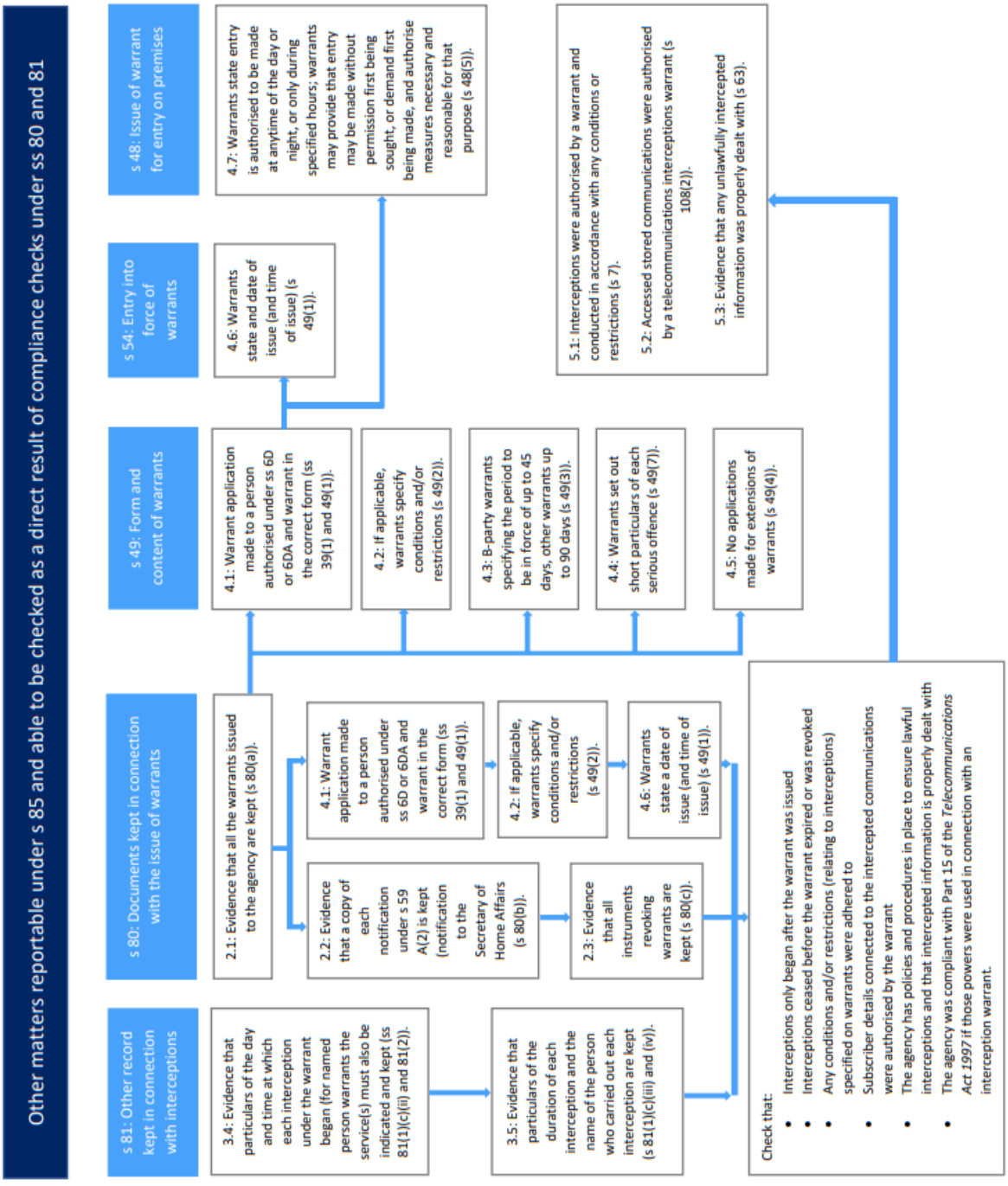


Figure 2: Other Matters Reportable Under Section 85



CHAPTER 3 – 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 makes it an offence to access stored communications except in limited circumstances. Authorities and bodies that are criminal law-enforcement agencies under the TIA Act can apply to an issuing authority[17] for a stored communications warrant to investigate a 'serious contravention' as defined in the TIA Act.

Definition

'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.

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, and
- offences punishable by a fine of at least 180 penalty units ($39,960 during the reporting period) for individuals or 900 penalty units ($199,800 during the reporting period) for non-individuals such as corporations.

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

This information is presented in **Table 25**. In 2021–22, 807 stored communications warrants were issued, representing a decrease of 191 from the previously 998 stored communications warrants issued in 2020–21.

[17] An issuing authority is defined at section 6DB of the TIA Act and means a judge, magistrate or an AAT member who is enrolled as a legal practitioner for at least 5 years, and who has been appointed by the Attorney-General.

Table 25: Applications, telephone applications and renewal applications for stored communications warrants – paragraphs 162(1)(a)-(b), 162(2)(a)-(b) and 162(2)(c)

Agency	Relevant statistics	Applications for stored communications warrants		Telephone applications for stored communications warrants		Renewal applications for stored communications warrants	
		20/21	21/22	20/21	21/22	20/21	21/22
ACCC	Made	-	1	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	-	1	-	-	-	-
ACIC	Made	1	-	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	1	-	-	-	-	-
AFP	Made	83	36	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	83	36	-	-	-	-
Home Affairs	Made	1	-	-	-	-	-
	Withdrawn	-	-	-	-	-	-
	Issued	1	-	-	-	-	-
IBAC	Made	-	8	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	-	8	-	-	-	-
ICAC (SA)	Made	2	-	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	2	-	-	-	-	-
LECC	Made	9	-	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	9	-	-	-	-	-
NSW CC	Made	-	2	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	-	2	-	-	-	-
NSW Police	Made	489	406	6	-	-	-
	Refused	-	-	-	-	-	-
	Issued	489	406	6	-	-	-
NT Police	Made	1	5	-	-	-	-
	Refused	-	1	-	-	-	-
	Issued	1	4	-	-	-	-
QLD CCC	Made	1	-	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	1	-	-	-	-	-
QLD Police	Made	129	98	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	129	98	-	-	-	-
SA Police	Made	47	16	-	-	-	-
	Refused	-	-	-	-	-	-

Agency	Relevant statistics	Applications for stored communications warrants		Telephone applications for stored communications warrants		Renewal applications for stored communications warrants	
		20/21	21/22	20/21	21/22	20/21	21/22
TAS Police	Issued	47	16	-	-	-	-
	Made	40	29	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	40	29	-	-	-	-
VIC Police	Made	108	125	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	108	125	-	-	-	-
WA Police	Made	87	82	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	87	82	-	-	-	-
TOTAL	**Made**	**998**	**808**	**6**	**0**	**0**	**0**
	Refused / Withdrawn	**0**	**1**	**0**	**0**	**0**	**0**
	Issued	**998**	**807**	**6**	**0**	**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 during the year specified conditions or restrictions relating to access to stored communications under warrants.

This information is presented in **Table 26**. In 2021–22, 466 stored communications warrants were subject to conditions or restrictions, this is a decrease of 66 warrants compared to 2020–21.

Table 26: Stored communications warrants subject to conditions or restrictions – paragraph 162(2)(d)

Agency	20/21	21/22
AFP	1	14
NSW CC	-	1
NSW Police	489	406
SA Police	41	16
TAS Police	1	29
TOTAL	**532**	**466**

Effectiveness of stored communications warrants

Section 163 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.

This information is presented in **Table 27**. In 2021–22, criminal law-enforcement agencies made 357 arrests, conducted 594 proceedings, and obtained 389 convictions involving evidence obtained under stored communications warrants.

Table 27: Arrests, proceedings and convictions made on the basis of lawfully accessed information – paragraphs 163(a)-(b)

Agency	Arrests		Proceedings		Convictions	
	20/21	21/22	20/21	21/22	20/21	21/22
ACIC	1	-	-	1	-	1
AFP	12	5	14	10	2	11
NSW Police	288	219	692	549	249	332
QLD Police	91	78	7	10	7	10
SA Police	8	-	-	5	6	8
TAS Police	5	1	10	-	10	-
VIC Police	65	54	17	19	102	27
TOTAL	**470**	**357**	**740**	**594**	**376**	**389**

Care should be taken in interpreting **Table 27** 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 requires a carrier 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 stored 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 stored 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 a serious contravention of foreign laws. Only the AFP may give foreign preservation notices.

An issuing agency that has given a domestic preservation notice may revoke the notice at any time, but must revoke the notice if the grounds on which the notice was issued ceases to exist.

The AFP must revoke a foreign preservation notice if either the foreign entity did not make a request for access to stored communications within 180 days, or a request is made but the Attorney-General refuses access to the communication.

Revocation is achieved through giving notice of revocation to the carrier.

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

This information is presented in **Table 28**. In 2021–22, 1,602 domestic preservation notices were given. This is a decrease of 488 notices on the 2,090 given in 2020–21.

Table 28: Domestic preservation notices – subsection 161A(1)

Agency	Domestic preservation notices issued		Domestic preservation revocation notices issued	
	20/21	21/22	20/21	21/22
ACCC	6	1	8	-
ACIC	4	-	1	-
ACLEI	1	2	-	1
AFP	474	252	151	136
CCC (WA)	-	5	-	-
Home Affairs	2	-	2	-
IBAC	2	8	-	2
ICAC (NSW)	1	-	-	-
ICAC (SA)	14	2	7	2
LECC	17	1	5	1
NSW CC	4	2	1	-
NSW Police	598	599	95	131
NT Police	57	27	45	6
QLD CCC	62	10	47	10
QLD Police	334	261	116	93
SA Police	127	70	77	52
TAS Police	76	58	35	24
VIC Police	159	150	23	29
WA Police	152	154	78	64
TOTAL	**2,090**[18]	**1,602**	**691**	**551**

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 2021–22, no foreign preservation notices or revocation notices were given.

Table 29: Foreign preservation notices – subsection 161A(2)

Agency	Foreign preservation notices given		Foreign preservation revocation notices given	
	20/21	21/22	20/21	21/22
AFP	1	-	-	-

[18] Correction for 2020-21: ACLEI figures relating to the number of domestic preservation notices issued have been amended due to a reporting error in the 2020-21 TIA Act Annual Report. As such, the total figures have also been amended. Appendix D provides both the original figures reported for the 2020-21 period, and the amended figures identified and amended by ACLEI.

International assistance

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

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

(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.

Paragraphs 162(1)(c) and 162(2)(ba) provide that this report must set out the number of stored communications warrant applications made as a result of international assistance applications.

Paragraphs 162(1)(d) and 162(2)(e) provide that this report must list, for each international offence in respect of which a stored communications warrant application was made 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, or substantially similar nature to, the international offence.

This information is presented in **Table 30**. In 2021–22, no agencies made applications for stored communications warrant as a result of an international assistance applications.

Table 30: Applications for stored communications warrants as a result of international assistance applications – paragraphs 162(1)(c) and 162(2)(ba)

Agency	Relevant statistics	Applications for stored communications warrants	
		20/21	21/22
AFP	Made	5	-
	Refused	-	-
	Issued	5	-

Paragraph 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
- the International Criminal Court, and
- a War Crimes Tribunal.

In 2021–22, there were no occasions in which lawfully accessed information or stored communications warrant information was provided to a foreign country, the International Criminal Court or a War Crimes Tribunal. There was no change from 2020-21.

Ombudsman inspection report

The Ombudsman inspects the preservation notices and stored communications access records of all criminal law-enforcement agencies. Under section 186J of the TIA Act, the Ombudsman continues to have a statutory obligation to report on the results of these inspections to the Attorney-General.

The Attorney-General 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 3 and 4 of the TIA Act can be found at www.ombudsman.gov.au.

CHAPTER 4 – 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) or customer information about a service, such as customer name, address or billing details.

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

Definition

'Enforcement agency' is defined as a criminal law-enforcement agency or an authority or body for which a declaration is in force. A declaration remains in force for 40 Parliamentary sitting days. On 9 February 2022, the NSW Department of Communities and Justice was declared an enforcement agency.

Telecommunications data is often the first source of lead information for 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 authorised by a senior officer of the relevant enforcement agency.

Definition

'Existing data', also known as 'historical data', is information that is already in existence when an authorisation for disclosure is received by a 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 reasonably necessary for the investigation of an offence punishable by imprisonment for at least 3 years. A prospective data authorisation comes into force once the relevant carrier receives the request and is effective for a maximum period of 45 days.

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 the disclosure is reasonably necessary for the enforcement of the criminal law.

Paragraph 186(1)(a) and subsection 186(2) of the TIA Act provides that this report must set out the number of authorisations made under section 178 of the TIA Act by agencies during the year.

This information is provided in **Table 31**. In 2021–22, there were 304,652 authorisations made by agencies under section 178 of the TIA Act. This is a decrease of 8,654 from the 313,306 authorisations made in 2020–21.

Table 31: Authorisations made by an enforcement agency for access to existing information or documents for the enforcement of the criminal law – paragraph 186(1)(a)

Agency	Authorisations	
	20/21	21/22
ACCC	93	34
ACIC	3,957	4,582
ACLEI	175	265
AFP	19,184[19]	14,856
ASIC	536	455
CCC (WA)	174	53
Home Affairs	5,565	3,409
IBAC	307	337
ICAC (NSW)	149	201
ICAC (SA)	175	79
LECC	766	517
NSW CC	3,538	3,007
NSW Police	103,056[20]	103,239
NT Police	1,991	2,325
QLD CCC	788	595
QLD Police	25,764[21]	26,051

[19] Correction for 2020-21: AFP figures relating to authorisations made in relation to the enforcement of the criminal law have been amended due to a reporting error in the 2020-21 Annual Report. As such, the figures have been amended. Appendix D provides both the original figures reported for the 2020-21 period, and the amended figures as identified and amended by AFP.
[20] Correction for 2020-21: NSW Police figures relating to authorisations made in relation to the enforcement of the criminal law have been amended due to a reporting error in the 2020-21 Annual Report. As such, the figures have been amended. Appendix D provides both the original figures reported for the 2019-20 period, and the amended figures identified and amended by NSW Police.
[21] Correction for 2020-21: QLD Police figures relating to authorisations made in relation to the enforcement of the criminal law have been amended due to a reporting error in the 2020-21 TIA Act Annual Report. As such, the figures have been amended. Appendix D provides both the original figures reported for 2020-21, and the amended figures as identified and amended by QLD Police.

Agency	Authorisations	
	20/21	21/22
SA Police	5,656	4,501
TAS Police	5,845	4,821
VIC Police	109,381	108,043
WA Police	26,206	27,282
TOTAL	313,306[22]	304,652

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 the disclosure is reasonably necessary for the purposes of finding a person that has been reported missing.

Paragraph 186(1)(aa) and subsection 186(2) of the TIA Act provides that this report must set out the number of authorisations made under section 178A by agencies during the year.

This information is presented in **Table 32**. In 2021–22, there were 4,207 authorisations made by agencies under section 178A of the TIA Act. This is an increase of 694 from the 3,513 authorisations made in 2020–21.

Table 32: Authorisations made for access to existing information or documents for the location of missing persons – paragraph 186(1)(aa)

Agency	Authorisations	
	20/21	21/22
AFP	76[23]	59
NSW Police	2,121	2,515
NT Police	21	35
QLD Police	260[24]	510
SA Police	83	49
TAS Police	13	83
VIC Police	728	779
WA Police	211	177
TOTAL	3,513[25]	4,207

[22] Correction for 2020-21: AFP, NSW Police, and QLD Police figures relating to authorisations made for the enforcement of the criminal law have been amended due to reporting errors in the 2020-21 TIA Act Annual Report. As such, the total figures have also been amended. Appendix D provides both the original figures reported for 2020-21, and the amended figures identified and amended by these agencies.
[23] Correction for 2020-21: AFP figures relating to authorisations for location of a missing person have been amended due to reporting errors in the 2020-21 TIA Act Annual Report. As such, figures have been amended. Appendix D provides both the original figures reported for 2020-21, and the amended figures as identified and corrected by AFP.
[24] Correction for 2020-21: AFP figures relating to authorisations for location of a missing person have been amended due to reporting errors in the 2020-21 TIA Act Annual Report. As such, figures have been amended. Appendix D provides both the original figures reported for 2020-21, and the amended figures as identified and corrected by QLD Police.
[25] Correction for 2020-21: AFP and QLD Police figures relating to authorisations for location of a missing person have been amended due to reporting errors in the 2020-21 TIA Act Annual Report. As such, the total figures have also been amended.

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 the disclosure 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) and subsection 186(2) of the TIA Act provides that this report must set out the number of authorisations made under section 179 by agencies during the year.

This information is presented in **Table 33**. In 2021–22, there were 1,734 authorisations made by agencies under section 179 of the TIA Act, this is an increase of 258 from the 1,476 authorisations made in 2020–21.

Table 33: Authorisations made by enforcement agency for access to existing information or documents for the enforcement of a law imposing a pecuniary penalty or protection of the public revenue – paragraph 186(1)(b)

Agency	Authorisations	
	20/21	21/22
ACCC	24	5
AFP	26[26]	4
ASIC	86	51
Home Affairs	18	44
NSW Police	1,256	1,568
NT Police	45	35
QLD Police	7	-
TAS Police	8	9
WA Police	6	18
TOTAL	**1,476[27]**	**1,734**

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 data if they are satisfied the disclosure 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.

Appendix D provides both the original figures reported for 2020-21, and the amended figures identified and amended by these agencies.

[26] Correction for 2020-21: AFP figures relating to authorisations for imposing a pecuniary penalty have been amended due to reporting errors in the 2020-21 TIA Act Annual Report. As such, figures have been amended. Appendix D provides both the original figures reported for 2020-21, and the amended figures as identified and corrected by AFP.

[27] Correction for 2020-21: AFP figures relating to authorisations for imposing a pecuniary penalty have been amended due to reporting errors in the 2020-21 TIA Act Annual Report. As such, the total figures have also been amended. Appendix D provides both the original figures reported for 2020-21, and the amended figures identified and amended by AFP.

Paragraph 186(1)(c) and subsection 186(2) of the TIA Act provides that this report must set out the number of authorisations made under section 180 of the TIA Act by agencies during the year. This information is presented in **Table 34**.

In 2021–22, there were 38,097 prospective data authorisations made by agencies under section 180 of the TIA Act. This is a decrease of 1,192 on the 39,289 authorisations made in 2020–21.

Table 34: Total number of prospective data authorisations made – paragraph 186(1)(c)

Agency	Number of authorisations made	
	20/21	21/22
ACCC	-	3
ACIC	1,116	1,220
ACLEI	40	75
AFP	6,591	5,190
ASIC	124	89
CCC (WA)	85	49
Home Affairs	416	318
IBAC	244	158
ICAC (NSW)	19	4
ICAC (SA)	52	5
LECC	130	107
NSW CC	1,594	926
NSW Police	1,479	1,984
NT Police	340	449
QLD CCC	244	203
QLD Police	4348	4,131
SA Police	471	324
TAS Police	114	117
VIC Police	17,911	18,936
WA Police	3,971	3,809
TOTAL	**39,289**	**38,097**

Data authorisations for foreign law enforcement

Division 4A of Part 4-1 of the TIA Act provides that the AFP may authorise the disclosure of telecommunications data where the disclosure is reasonably necessary for:

- the enforcement of the criminal law of a foreign country
- an investigation or prosecution of a crime within the jurisdiction of the International Criminal Court, or
- an investigation or prosecution of a War Crimes Tribunal offence.

However, for the disclosure of prospective telecommunications data, the Attorney-General must first give an authorisation 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*.

The AFP may authorise the disclosure of telecommunications data obtained under an authorisation for foreign law enforcement for the performance by ASIO of its functions, the enforcement of the criminal law or a law imposing a pecuniary penalty, the protection of the public revenue or the purpose of Division 105A of the *Criminal Code*, relating to post-sentence orders.

Paragraph 186(1)(ca) and subsection 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 of the TIA Act during the year.

Offences for which authorisations were made

Paragraph 186(1)(e) and subsection 186(2) 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 of the TIA Act. Information relating to sections 178, 179 and 180 are presented in **Tables 35, 36 and 37** respectively.

Under section 178A of the TIA Act, 4,208 requests were made in relation to missing persons.

The total number of offences is typically larger than the total number of authorisations issued, as an authorisation can be issued to investigate more than one offence.

Table 35: Offences for which authorisations were made under section 178 to access existing data to enforce the criminal law – paragraph 186(1)(e)[28]

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	-	-	-	205	-	-	-	-	2	-	-	67	7,426	102	-	2,627	214	419	6,448	2,732	**20,242**
Acts – injury	-	-	-	82	-	-	-	-	-	-	1	-	4,859	58	-	2	116	44	4,712	1,423	**11,297**
Bribery or corruption	-	-	338	57	-	48	-	315	49	75	334	-	-	3	78	2	23	-	-	111	**1,433**
Cartel offences	34	-	-	-	-	-	-	-	-	-	-	-	6	-	-	-	-	-	-	-	**40**
Conspire	-	17	-	67	14	-	-	-	-	2	-	-	202	2	-	6	28	-	248	30	**616**
Cybercrime	-	-	-	809	28	-	-	-	-	-	-	-	2,226	34	5	914	2	68	1,620	296	**6,002**
Dangerous acts	-	-	-	38	-	-	-	-	-	-	-	-	820	54	-	1,248	293	30	2,350	455	**5,288**
Fraud	-	-	-	966	451	-	103	6	150	2	121	291	13,121	74	1	544	346	132	9,850	1,348	**27,506**
Homicide	-	1	-	1,184	-	-	-	-	-	-	-	465	16,671	122	-	1,749	817	649	6,108	1,345	**29,111**
Illicit drug offences	-	109	8	6,155	-	-	1,656	3	-	-	51	1,806	22,231	1,215	283	3,647	1,258	2,365	18,810	5,988	**65,585**
Loss of life	-	-	-	51	-	-	-	-	-	-	-	1	488	7	-	834	22	11	322	3	**1,739**
Miscellaneous	-	12	-	194	11	1	1,263	-	-	-	4	3	4,915	83	228	6,363	22	102	229	412	**13,842**
Justice procedures	-	-	55	236	-	-	-	13	-	-	6	1	692	73	-	-	52	64	9,601	1,000	**11,793**
Organised offences	-	40	4	313	-	4	-	-	-	-	-	-	2,101	1	-	3	9	3	3	448	**2,929**

[28] 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
Pecuniary penalty	-	-	-	3	4	-	-	-	-	-	-	-	768	-	-	-	-	-	-	-	**775**
Public revenue	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	16	**17**
People smuggling	-	-	-	108	-	-	-	-	-	-	-	-	4	2	-	-	-	-	-	-	**114**
Weapons	-	-	-	125	-	-	150	-	-	-	-	57	1,273	-	-	92	114	53	2,994	63	**4,921**
Property damage	-	-	-	36	-	-	-	-	-	-	-	-	1,630	12	-	-	31	31	2,863	19	**4,622**
Public order offences	-	-	-	-	-	-	-	-	-	-	-	-	527	-	-	37	40	-	580	171	**1,355**
Robbery	-	-	-	92	-	-	-	-	-	-		-	6,786	29	-	1,456	269	69	7,544	2,452	**18,697**
Serious damage	-	-	-	23	-	-	-	-	-	-	-	-	417	18	-	708	33	54	7	207	**1,467**
Sexual assault	-	-	-	2,852	-	-	1	-	-	-	-	-	8,021	395	-	2,047	355	113	5,996	1,537	**21,317**
Special ACC investigation	-	4,426	-	-	-	-	-	-	-	-	-	-	-	-	-	29	1	-	-	-	**4,456**
Terrorism offences	-	-	-	481	-	-	-	-	-	-	-	315	182	2	-	-	25	-	331	142	**1,478**
Theft	-	-	-	610	-	-	236	-	-	-	-	1	4,955	10	-	1,227	80	349	10,340	2,183	**19,991**
Traffic	-	-	-	16	-	-	-	-	-		-	-	638	2	-	258	4	30	1,151	248	**2,347**
Unlawful entry	-	-	-	153	-	-	-	-	-	-	-	-	2,280	27	-	1,690	347	137	15,936	4,653	**25,223**
TOTAL	**34**	**4,605**	**406**	**14,856**	**508**	**53**	**3,409**	**337**	**201**	**79**	**517**	**3,007**	**103,239**	**2,325**	**595**	**25,483**	**4,501**	**4,723**	**108,043**	**27,282**	**304,203**

Table 36: Matters for 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	TAS Police	WA Police	TOTAL
Abduction	-	-	-	-	12	-	-	-	**12**
Acts – injury	-	-	-	-	12	-	-	-	**12**
Cartel offences	2	-	-	-	-	-	-	-	**2**
Cybercrime	-	-	7	-	24	-	-	-	**31**
Dangerous acts	-	-	-	-	7	10	-	-	**17**
Fraud	-	-	44	-	22	1	-	2	**69**
Homicide	-	-	-	-	182	-	-	-	**182**
Illicit drug offences	-	-	-	12	97	-	-	-	**109**
Loss of life	-	-	-	-	7	2	-	-	**9**
Miscellaneous	-	-	2	4	47	6	1	-	**60**
Justice procedures	-	-	-	-	5	16	2	4	**27**
Organised offences	-	-	-	-	44	-	-	-	**44**
Pecuniary penalty	3	3	6	28	419	-	6	-	**465**
Public revenue	-	1	-	-	-	-	-	-	**1**
Weapons	-	-	-	-	4	-	-	-	**4**
Property damage	-	-	-	-	2	-	-	-	**2**

Categories of offences	ACCC	AFP	ASIC	Home Affairs	NSW Police	NT Police	TAS Police	WA Police	TOTAL
Public order offences	-	-	-	-	3	-	-	1	**4**
Robbery	-	-	-	-	508	-	-	-	**508**
Serious damage	-	-	-	-	-	-	-	-	**-**
Sexual assault	-	-	-	-	39	-	-	-	**39**
Theft	-	-	-	-	95	-	-	-	**95**
Traffic	-	-	-	-	17	-	-	11	**28**
Unlawful entry	-	-	-	-	22	-	-	-	**22**
TOTAL	**5**	**4**	**59**	**44**	**1,568**	**35**	**9**	**18**	**1,742**

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	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	-	-	-	26	-	-	-	-	-	-	-	5	101	1	-	367	20	5	1,121	95	**1,741**
Acts – injury	-	-	-	27	-	-	-	-	-	-	-	-	240	8	-	43	25	-	1,331	191	**1,865**
Bribery or corruption	-	-	85	72	-	42	-	158	-	5	79	-	-	-	15	2	-	-	21	8	**487**
Cartel offences	3	-	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	-	-	**4**
Conspire	-	37	-	23	6	-	-	-	-	-	-	-	12	-	-	5	2	-	36	-	**121**
Cybercrime	-	-	-	184	7	-	-	-	-	-	-	-	8	2	-	12	-	-	49	-	**262**
Dangerous acts	-	-	-	16	-	-	-	-	-	-	-	-	6	3	-	45	7	2	515	-	**594**
Fraud	-	4	-	298	89	-	34	-	4	-	20	102	84	13	-	98	-	-	642	198	**1,586**
Homicide	-	-	-	200	-	-	-	-	-	-	-	107	90	5	-	306	20	12	719	58	**1,517**
Illicit drug offences	-	377	-	2,774	-	-	76	-	-	-	8	605	695	349	156	2,147	124	77	4,116	1,364	**12,868**
Loss of life	-	-	-	21	-	-	-	-	-	-	-	-	38	-	-	2	7	-	4	-	**72**
Miscellaneous	-	3	-	67	5	-	114	-	-	-	-	-	146	7	32	48	4	1	25	190	**642**
Justice procedures	-	-	-	102	-	-	-	-	-	-	-	-	22	11	-	-	-	1	1,269	96	**1,501**
Organised offences	-	375	-	665	-	7	-	-	-	-	-	-	19	-	-	6	2	-	3	-	**1,077**

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
Pecuniary penalty	-	332	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**332**
Public revenue	-	32	-	1	-	-	-	-	-	-	-	-	8	-	-	-	-	-	-	-	**41**
People smuggling	-	-	-	35	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**35**
Weapons	-	1	-	55	-	-	76	-	-	-	-	30	132	-	-	140	18	1	966	36	**1,455**
Property damage	-	-	-	15	-	-	-	-	-	-	-	-	18	2	-	-	-	-	307	66	**408**
Public order offences	-	-	-	-	-	-	-	-	-	-	-	-	5	-	-	-	-	1	108	44	**158**
Robbery	-	-	-	26	-	-	-	-	-	-	-	-	130	3	-	269	13	7	1,304	248	**2,000**
Serious damage	-	-	-	8	-	-	-	-	-	-	-	-	8	-	-	76	-	-	27	-	**119**
Sexual assault	-	-	-	285	-	-	-	-	-	-	-	-	72	32	-	89	32	1	698	82	**1,291**
Special ACC investigation	-	66	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**66**
Terrorism offences	-	-	-	86	-	-	-	-	-	-	-	77	6	-	-	5	-	-	70	4	**248**
Theft	-	-	-	243	-	-	18	-	-	-	-	-	106	2	-	180	-	6	2,314	370	**3,239**
Traffic	-	-	-	12	-	-	-	-	-	-	-	-	1	-	-	-	2	-	138	-	**153**
Unlawful entry	-	-	-	52	-	-	-	-	-	-	-	-	36	11	-	291	48	3	3,153	759	**4,353**
TOTAL	**3**	**1,227**	**85**	**5,293**	**107**	**49**	**318**	**158**	**4**	**5**	**107**	**926**	**1,984**	**449**	**203**	**4,131**	**324**	**117**	**18,936**	**3,809**	**38,235**

Age of data under disclosure

Paragraph 186(1)(f) and subsection 186(2) of the TIA Act provide that this report must set out the lengths of time for which information or documents covered by data authorisations had been held by a service provider before the authorisations for that information were made.

This information is provided in **Table 38**. 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, in accordance with subsection 180(1C) of the TIA Act.

In 2021–22, there were 259,235 authorisations 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,[29] which have been recorded as '0' months old and are included in the 0–3 month field.

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	2	-	5	9	1	2	-	9	11	**39**
ACIC	3,705	412	211	71	63	29	30	13	59	**4,593**
ACLEI	275	37	28	11	3	3	5	6	21	**389**
AFP	6,319	3,510	1,550	900	1,008	245	292	183	912	**14,919**
ASIC	299	55	27	43	24	1	3	13	41	**506**
CCC (WA)	46	-	-	-	-	1	-	-	6	**53**
Home Affairs	2,228	527	302	86	134	35	17	39	85	**3,453**
IBAC	263	10	13	4	4	1	4	5	33	**337**
ICAC (NSW)	13	1	-	2	1	5	5	2	172	**201**
ICAC (SA)	25	7	-	4	6	13	1	-	23	**79**
LECC	389	39	24	19	4	15	6	8	13	**517**
NSW CC	2,082	161	180	137	133	72	50	86	106	**3,007**
NSW Police	92,349	4,959	2,782	1,680	1,629	867	485	310	2,261	**107,322**
NT Police	2,028	80	25	18	14	7	7	6	211	**2,396**
QLD CCC	328	45	49	66	22	17	19	7	42	**595**
QLD Police	22,172	1,561	824	472	304	202	187	179	657	**26,558**

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

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
SA Police	3,133	466	269	190	108	126	89	65	428	**4,874**
TAS Police	4,275	221	71	64	32	17	30	15	188	**4,913**
VIC Police	97,835	4,738	2,301	1,113	845	643	416	308	623	**108,822**
WA Police	21,469	2,519	1,043	620	519	221	214	158	714	**27,477**
TOTAL	**259,235**	**19,348**	**9,704**	**5,509**	**4,854**	**2,522**	**1,860**	**1,412**	**6,606**	**311,050**

Types of data retained

Paragraphs 186(1)(g)-(h) and subsection 186(2) 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 about 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. 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.

Table 39: Types of retained data disclosed in authorisations – paragraphs 186(1)(g) and 186(1)(h)[30]

Agency	Item 1: subscriber data	Items 2 – 6: traffic data
ACCC	19	20
ACIC	2,857	1,736
ACLEI	21	244
AFP	11,834	3,085
ASIC	249	257
CCC (WA)	35	18
Home Affairs	2,648	1,613
IBAC	230	123
ICAC (NSW)	88	113
ICAC (SA)	39	40
LECC	381	243
NSW CC	1,275	1,732
NSW Police	73,647	33,672
NT Police	1,972	424
QLD CCC	437	158
QLD Police	18,399	6,829
SA Police	2,671	1,879
TAS Police	4,078	869
VIC Police	61,070	47,752
WA Police	20,124	7,353
TOTAL	**202,074**	**108,160**

[30] An agency can request both types of data in a single request.

Journalist information warrants

The journalist information warrant (JIW) scheme requires agencies to obtain a journalist information warrant prior to authorising the disclosure of telecommunications data relating to journalist or their employer, for the purpose of identifying a journalist's source.

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.

In 2021–22, no JIWs were issued and no authorisations were made under a JIW. This is consistent with 2020–21.

To issue a JIW, the issuing authority must, amongst other things, have regard to any submissions made by a Public Interest Advocate (PIA). The Prime Minister may declare the following persons to be PIAs:

- a King's Counsel or Senior Counsel who has been cleared for security purposes to a level the Prime Minister considers to be appropriate, or
- a former Judge.

A PIA may make a submission to an issuing authority (or the Attorney-General in the case of ASIO) about matters relevant to a decision to issue, refuse, or specify conditions in a JIW. In the case of oral applications, they can attend the hearing of the application.

In August 2020, the PJCIS handed down its report on its Inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press. The PJCIS made a number of recommendations, including to require additional record-keeping and reporting requirements in respect of PIAs. Ahead of legislative amendments, the Government has included information about the number of PIAs, their location and qualification in **Table 40.**

Table 40: Public interest advocates

Public interest advocate	Location	Qualification
1	South Australia	Former Judge
2	Queensland	Former Judge

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. This information is set out in **Table 41**.

Table 41 further sets out the costs recovered from criminal law-enforcement agencies for the purpose of complying with their data retention obligations.

Table 41: Industry capital cost of data retention – section 187P

Financial year	Data retention compliance cost (GST inclusive) (*exclusive of data retention industry grants*)	Costs recovered from criminal law-enforcement agencies (GST inclusive)
2020–21	$25,262,114.03	$13,385,407.50
2021-22	$28,136,658.54	$14,228,772.50

CHAPTER 5 – INTERNATIONAL PRODUCTION ORDERS

Schedule 1 to the TIA Act enables Australian agencies to obtain international production orders (IPOs) for interception, stored communications, and telecommunications data from foreign communication providers. IPOs may be served directly to prescribed communication providers in foreign countries with which Australia has a designated international agreement.

Definition

'Prescribed communication provider' is defined in clause 2 of Schedule 1 to the TIA Act as:

- a network entity, or
- a transmission service provider, or
- a message/call application service provider, or
- a storage/back-up service provider, or
- a general electronic service provider.

Agencies who can obtain warrants and authorise the disclosure of telecommunications data under Chapters 2 to 4 of the TIA Act can obtain IPOs for the equivalent power.

Paragraph 131(1)(a) of Schedule 1 provides that this report must set out information about IPOs relating to each agency. Due to the absence of a designated international agreement in 2021-2022, no IPOs were issued in this reporting period.

No IPOs were issued in 2021-22. The process to establish a designated international agreement is still underway (a requirement of Schedule 1 to the TIA Act).

Paragraph 131(1)(b) of Schedule 1 provides that this report must set out information relating to the Australian Designated Authority. **Table 42** reflects that no IPOs were issued in 2021-2022.

Table 42: Annual report by the Australian Designated Authority – clause 131

Australian Designated Authority 2021-22 Annual Report	
Reporting item	**Number for each agency**
International production orders that were given by the Australian Designated Authority to prescribed communications providers (clause 130(1)(a)(i))	**0**
International production orders relating to interception that were given by the Australian Designated Authority to prescribed communications providers (clause 130(1)(a)(ii))	**0**
International production orders relating to stored communications that were given by the Australian Designated Authority to prescribed communications providers (clause 130(1)(a)(ii))	**0**
International production orders relating to telecommunications data that were given by the Australian Designated Authority to prescribed communications providers (clause 130(1)(a)(ii))	**0**
International production orders that invoked each designated international agreement that were given by	**0**

Australian Designated Authority 2021-22 Annual Report	
the Australian Designated Authority to prescribed communications providers (clause 130(1)(a)(iii))	
International production orders to which subparagraph 30(2)(g)(ii) or (h)(ii) applied to that were given by the Australian Designated Authority to prescribed communications providers (clause 130(1)(b))	**0**
International production orders to which subparagraph 60(2)(g)(ii) or (h)(ii) applied that were given by the Australian Designated Authority to prescribed communications providers (clause 130(1)(c))	**0**
International production orders that were cancelled by the Australian Designated Authority under clause 111 (clause 130(1)(d))	**0**
International production orders that were cancelled by the Australian Designated Authority under clause 122 (clause 130(1)(e))	**0**
Instruments of revocation of international production orders that were given by the Australian Designated Authority to prescribed communications providers (clause 130(1)(f))	**0**
International production orders for which objections were received by the Australian Designated Authority under clause 121 (clause 130(1)(g)(i))	**0**
International production orders relating to interception for which objections were received by the Australian Designated Authority under clause 121 (clause 130(1)(g)(ii))	**0**
International production orders relating to stored communications for which objections were received by the Australian Designated Authority under clause 121 (clause 130(1)(g)(ii))	**0**
International production orders relating to telecommunications data for which objections were received by the Australian Designated Authority under clause 121 (clause 130(1)(g)(ii))	**0**
International production orders that invoked each designated international agreement for which one or more objections were received by the Australian Designated Authority under clause 121 (clause 130(1)(g)(iii))	**0**

CHAPTER 6 – INDUSTRY ASSISTANCE

Part 15 of the Telecommunications Act provides 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.

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.[31]
- **Technical Assistance Notice (TAN):** Agencies can require designated communications providers to give help where they already have the technical capability to do so.
- **Technical Capability Notice (TCN):** Agencies can require designated communication providers to give help, including in circumstances where they may not have the technical capability to do so.

Table 43: Eligible agencies under Part 15 of the Telecommunications Act

Agency	Industry assistance powers available to agencies		
	TAR	TAN	TCN
Interception Agencies[32]	✓	✓	✓
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.

[31] Categories of designated communications providers and their eligible activities are at section 317C of the Telecommunications Act.
[32] 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, and
- providers may not be requested or required to implement or build on prevent rectification of, a system weakness in a form of electronic protection.

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
- prohibiting the doing of things that would otherwise require agencies to obtain a warrant or authorisation under the relevant law of the Commonwealth, States or Territories to authorise that act (such as a warrant under the TIA Act), and
- 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 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 2021–22, 30 TARs were given by interception agencies to designated communications providers. This increased by four from the previous year.[33]

No TANs or TCNs were given or sought by interception agencies.

Table 44: Technical Assistance Requests, Technical Assistance Notices, and Technical Capability Notices given – paragraphs 317ZS(1)(a)-(c) of the Telecommunications Act

Agency	Requests or notices given		
	Technical Assistance Request	Technical Assistance Notice	Technical Capability Notice
ACIC	4	-	-
AFP	2	-	-
NSW Police	21	-	-
VIC Police	3	-	-
TOTAL	**30**	**0**	**0**

Offences enforced through industry assistance

Paragraph 317ZS(1)(d) of the Telecommunications Act provides that if any TARs, TANs or TCNs were 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.

This information is provided in **Table 45**.

Table 45: Kinds of serious Australian offences enforced through Technical Assistance Requests – paragraphs 317ZS(1)(d) of the Telecommunications Act

Categories of offences	ACIC	AFP	NSW Police	VIC Police	TOTAL
ACIC investigation	4	-	-	-	**4**
Acts intendent to cause injury	-	-	1	-	**1**
Fraud, deception and related offences	-	-	1	-	**1**
Homicide and related offences	-	-	10	-	**10**
Illicit drug offences	-	-	7	2	**9**

[33] Correction for 2020-21: NSW Police figures relating to the number of TARs issued have been amended due to a reporting error in the 2020-21 TIA Act Annual Report. Appendix D provides both the original figures reported for the 2020-21 TIA Act Annual Report, and the amended figures identified and amended by NSW Police.

Categories of offences	ACIC	AFP	NSW Police	VIC Police	TOTAL
Sexual assault and related offences	-	2	-	1	**3**
Theft and related offences			1	-	**1**
Other serious Australian offences	-	-	1	-	**1**
TOTAL	**4**	**2**	**21**	**3**	**30**

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 Ombudsman or State and Territory oversight bodies.

The IGIS or the Ombudsman (as relevant) must be notified whenever a notice or request 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 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 on the outcome of their inspections.

The Ombudsman may also inspect agencies' records to ensure compliance with Part 15 of the Telecommunications Act. As the industry assistance measures complement powers under the TIA Act, the Ombudsman considers agency use of these powers collectively.

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 approval process ensures 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 TCN to an independent assessment panel consisting of a retired senior judge and a technical expert. This panel must consider whether proposed requirements will create a systemic vulnerability. Further, any decision to compel assistance may be challenged through judicial review.

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 IGIS. In the case of interception agencies, this is the 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.[34]

[34] Further information on Part 15 of the Telecommunications Act including detailed administrative guidance can be found on the AGD website, at <www.ag.gov.au>.

CHAPTER 7 – FURTHER INFORMATION

For further information about the TIA Act and Part 15 Telecommunications Act, please contact AGD:

Electronic Surveillance Section

Attorney-General's Department

3-5 NATIONAL CIRCUIT

BARTON ACT 2600

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

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

APPENDIX A – LISTS OF TABLES AND FIGURES

APPENDIX B – INTERCEPTION AGENCIES UNDER THE TIA ACT

Commonwealth agency or state eligible authority
Australian Commission for Law Enforcement Integrity
Australian Criminal Intelligence Commission
Australian Federal Police
Crime and Corruption Commission (Western Australia)
Crime and Corruption Commission (Queensland)
Independent Broad-based Anti-corruption Commission (Victoria)
Independent Commission Against Corruption (New South Wales)
New South Wales Crime Commission
New South Wales Police Force
Northern Territory Police Force
Law Enforcement Conduct Commission
Queensland Police Service
Independent Commissioner Against Corruption (South Australia)
South Australia Police
Tasmania Police
Victoria Police
Western Australia Police Force

APPENDIX C – CATEGORIES OF SERIOUS OFFENCES UNDER THE TIA ACT

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

APPENDIX D – UPDATE FIGURES FOR PREVIOUS REPORTING PERIODS

ACIC 2019-20

ACIC identified corrections regarding the number of telecommunications interception warrants issued by judges and AAT members. Below details both the original figures provided for the 2019-20 report, and the amended figures as identified and corrected.

Number of telecommunications interception warrants issued by Federal Court judges, Family Court judges, Federal Circuit Court judges and nominated AAT members – paragraph 103(ab)[35]

ACIC	Authorisations	
	19/20 Original	19/20 Updated
Family Court judges	10	21
Federal Circuit Court judges	6	6
Federal Court judges	92	1
Nominated AAT members	1	81
TOTAL	**109**	**109**

ACLEI

ACLEI identified corrections regarding the number of domestic preservation notices issued under the stored communications framework as reported in 2020-21, and the number of telecommunications data authorisations as reported in 2012-13 to 2015-16. Below details both the original figures included in the relevant annual reports, and the amended figures as identified and corrected.

Domestic preservation notices – subsection 161A(1)[36]

Agency	Domestic preservation notices issued	
	20/21 Original	20/21 Updated
ACLEI	3	1
TOTAL	**2,092**	**2,090**

[35] Correction refers to Table 3, page 13, 2019-20 TIA Act Annual Report.
[36] Corrections refer to Table 27, page 50, 2020-21 TIA Act Annual Report.

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)

Authorisations								
Agency	12/13 Original	12/13 Updated	13/14 Original	13/14 Updated	14/15 Original	14/15 Updated	15/16 Original	15/16 Updated
ACLEI	2,594[37]	190	2,244[38]	455	5,908[39]	762	2,123[40]	302
TOTAL	**312,929**	**310,525**	**314,587**	**312,798**	**341,597**	**336,451**	**325,807**	**323,986**

AFP 2016-17 to 2019-20

AFP identified corrections regarding access to telecommunications data for the 2016-17 to 2020-21 reporting periods. The below tables detail both the original figures provided for these previous annual reports 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							
	16/17 Original	16/17 Updated	17/18 Original	17/18 Updated	18/19 Original	18/19 Updated	19/20 Original	19/20 Updated
AFP	22,127[41]	22,129	19,432[42]	19,434	16,818[43]	16,795	18,534[44]	18,472
TOTAL	**293,069**	**293,071**	**295,795[45]**	**295,797**	**289,667[46]**	**289,644**	**307,018[47]**	**306,956**

Agency	Authorisations	
	20/21 Original	20/21 Updated
AFP	18,442[48]	19,184
TOTAL	**312,440**	**313,306[49]**

[37] Correction refers to Table 26, page 47, 2012-13 TIA Act Annual Report.
[38] Correction refers to Table 28, page 45, 2013-14 TIA Act Annual Report.
[39] Correction refers to Table 28, page 42, 2014-15 TIA Act Annual Report.
[40] Correction refers to Table 28, page 39, 2015-16 TIA Act Annual Report.
[41] Correction refers to Tables 28 and 29, pages 37 and 39, 2016-17 TIA Act Annual Report.
[42] Correction refers to Table 28, page 47, 2017-18 TIA Act Annual Report.
[43] Correction refers to Table 30, page 54, 2018-19 TIA Act Annual Report.
[44] Correction refers to Table 29, page 56, 2019-20 TIA Act Annual Report.
[45] This figure includes updates identified in Appendix D, page 87, 2019-20 TIA Act Annual Report.
[46] This figure includes updates identified in Appendix D, page 83, 2020-21 TIA Act Annual Report.
[47] This figure includes updates identified in Appendix D, page 81-83, 2020-21 TIA Act Annual Report.
[48] Correction refers to Table 30, pages 55 and 56, 2020-21 TIA Act Annual Report.
[49] This figure includes updates from NSW Police and QLD Police which are identified in this Appendix.

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

AFP	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
16/17 Original[50]	15,250	2,782	1,032	1,167	560	195	199	238	864	**22,287**
16/17 Updated	15,253	2,782	1,032	1,167	560	195	199	238	864	**22,290**
17/18 Original[51]	13,086	2,281	1,041	1,245	548	171	151	161	1,041	**19,725**
17/18 Updated	13,088	2,281	1,041	1,245	548	171	151	161	1,041	**19,727**
18/19 Original[52]	12,496	1,689	630	821	323	146	88	175	760	**17,128**
18/19 Updated	12,489	1,680	630	818	323	142	88	175	760	**17,105**
19/20 Original[53]	12,506	2,277	940	969	465	205	164	262	927	**18,715**
19/20 Updated	12,469	2,273	937	964	460	205	164	260	921	**18,653**
20/21 Original[54]	11,685	2,899	877	898	523	232	186	267	955	**18,522**
20/21 Updated	12,242	2,951	928	904	574	236	192	271	969	**19,267**

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

AFP	Item 1: subscriber data	Items 2 – 6: traffic data
16/17 Original[55]	6,179	16,086
16/17 Updated	6,181	16,087
17/18 Original[56]	15,057	4,578
17/18 Updated	15,059	4,578
18/19 Original[57]	12,687	4,305
18/19 Updated	12,664	4,305
19/20 Original[58]	14,689	4,026
19/20 Updated	14,670	3,983
20/21 Original[59]	15,190	3,332
20/21 Updated	15,932	3.335

[50] Corrections refer to Table 38, page 49, 2016-17 TIA Act Annual Report.
[51] Corrections refer to Table 36, page 60, 2017-18 TIA Act Annual Report.
[52] Corrections refer to Table 39, page 70, 2018-19 TIA Act Annual Report.
[53] Corrections refer to Table 38, page 72, 2019-20 TIA Act Annual Report.
[54] Corrections refer to Table 37, page 66, 2020-21 TIA Act Annual Report.
[55] Corrections refer to Table 39, page 50, 2016-17 TIA Act Annual Report.
[56] Correction refers to Table 37, page 61, 2017-18 TIA Act Annual Report.
[57] Correction refers to Table 40, page 71, 2018-19 TIA Act Annual Report.
[58] Corrections refer to Table 39, page 73, 2019-20 TIA Act Annual Report.
[59] Corrections refer to Table 38, page 68, 2020-21 TIA Act Annual Report.

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

Agency	Authorisations			
	16/17 Original	16/17 Updated	20/21 Original	20/21 Updated
AFP	91[60]	92	57[61]	76
TOTAL	**4,548**	**4,549**	**3,490**	**3,513**[62]

Offences for which authorisations were made to access existing data to enforce the criminal law – paragraph 186(1)(e)[63]

Categories of offences	16/17 Original	16/17 Updated
Illicit drug offences	12,362	12,364
TOTAL (AFP)	**22,127**	**22,129**

Offences for which authorisations were made to access existing data to enforce the criminal law – paragraph 186(1)(e)[64]

Categories of offences	17/18 Original	17/18 Updated
Dangerous acts	133	134
Traffic	57	58
TOTAL (AFP)	**15,425**	**15,427**

Offences for which authorisations were made to access existing data to enforce the criminal law – paragraph 186(1)(e)[65]

Categories of offences	18/19 Original	18/19 Updated
Homicide	414	410
Illicit drug offences	7,636	7,635
Justice procedures	317	315
Public order offences	14	13
Robbery	347	336
Unlawful entry	159	155
TOTAL (AFP)	**16,818**	**16,795**

[60] Corrections refer to Table 32, page 39, 2016-17 TIA Act Annual Report.
[61] Corrections refer to Table 31, page 56, 2020-21 TIA Act Annual Report.
[62] This figure includes updates from QLD Police which are identified in this Appendix.
[63] Corrections refer to Table 35, page 42, 2016-17 TIA Act Annual Report.
[64] Corrections refer to Table 33, pages 53, 2017-18 TIA Act Annual Report.
[65] Corrections refer to Table 35, pages 61-62, 2018-19 TIA Act Annual Report.

Offences for which authorisations were made to access existing data to enforce the criminal law – paragraph 186(1)(e)[66]

Categories of offences	19/20 Original	19/20 Updated
Abduction	414	408
Dangerous acts	61	58
Fraud	1,520	1,517
Illicit drug offences	8,518	8,498
Justice procedures	344	341
Robbery	317	316
Sexual assault	2,748	2,722
TOTAL (AFP)	**18,534**	**18,472**

Offences for which authorisations were made to access existing data to enforce the criminal law – paragraph 186(1)(e)[67]

Categories of offences	20/21 Original	20/21 Updated
Abduction	161	182
Acts – injury	56	89
Dangerous acts	31	37
Fraud	1,462	1,596
Homicide	468	748
Illicit drug offences	8,883	8,977
Miscellaneous	184	186
Justice procedures	410	437
Organised offences	290	293
Pecuniary penalty	36	37
Weapons	114	128
Property damage	26	27
Public order offences	1	2
Robbery	86	105
Sexual assault	3,166	3,213
Theft	869	888
Traffic	9	15
Unlawful entry	128	162
TOTAL (AFP)	**18,442**	**19,184**

[66] Corrections refer to Table 34, pages 63-64, 2019-20 TIA Act Annual Report.
[67] Corrections refer to Table 34, pages 60-61, 2020-21 TIA Act Annual Report.

Number of authorisations made by an enforcement agency for access to existing information or documents for the enforcement of a law imposing a pecuniary penalty or protection of the public revenue – paragraph 186(1)(b)[68]

Agency	Authorisations	
	20/21 Original	20/21 Updated
AFP	23	26
TOTAL	**1,473**	**1,476**

Matters for 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 public revenue – paragraph 186(1)(e)[69]

Categories of offences	20/21 Original	20/21 Updated
Pecuniary penalty	8	11
TOTAL (AFP)	**23**	**26**

NSW Police 2020-21

NSW Police identified corrections regarding access to telecommunications data and industry assistance for the 2020-21 reporting period. The below details both the original figures provided for the 2020-21 Annual Report and the amended figures as identified and corrected.

Number of authorisations made by an enforcement agency for access to existing information or documents for the enforcement of the criminal law – paragraph 186(1)(a) [70]

Agency	Authorisations	
	20/21 Original	20/21 Updated
NSW Police	103,051	103,056
TOTAL	**312,440**	**313,306[71]**

Offences for which authorisations were made under section 178 to access existing data to enforce the criminal law – paragraph 186(1)(e) [72]

Categories of offences	20/21 Original	20/21 Updated
Terrorism offences	196	201
TOTAL	**102,853**	**102,858**

[68] Correction refers to Table 32, page 57, 2020-21 TIA Act Annual Report.
[69] Corrections refer to Table 35, pages 62-63, 2020-21 TIA Act Annual Report.
[70] Corrections refer to Table 30, page 55-56, 2020-21 TIA Act Annual Report.
[71] This figure includes updates from AFP and QLD Police which are identified in this Appendix.
[72] Corrections refer to Table 34, page 61, 2020-21 TIA Act Annual Report.

Periods for which retained data was held by carrier before authorised disclosure – paragraph 186(1)(f)[73]

NSW 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
20/21 Original	95,306	4,060	1,838	1,816	694	564	284	325	1,541	**106,428**
20/21 Updated	95,311	4,060	1,838	1,816	694	564	284	325	1,541	**106,433**

Types of retained data disclosed in authorisations – paragraph 186(1)(g) and 186(1)(h)[74]

NSW Police	Item 1: subscriber data	Items 2 – 6: traffic data
20/21 Original	72,763	33,665
20/21 Updated	72,768	33,665

Number of Technical Assistance Requests, Technical Assistance Notices, and Technical Capability Notices given between 1 July 2020 and June 2021 – paragraphs 317ZS(1)(a)-(c) of the Telecommunications Act[75]

NSW Police	Requests or notices given			
	Technical Assistance Request	Technical Assistance Notice	Technical Capability Notice	TOTAL
20/21 Original	16	1	-	**17**
20/21 Updated	17	1	-	**18**

Kinds of serious Australian offences enforced through Technical Assistance Requests - paragraph 317ZS(1)(d) of the Telecommunications Act[76]

Categories of offences	20/21 NSW Police Original	20/21 NSW Police Updated
Robbery	-	1

[73] Correction refers to Table 37, page 67, 2020-21 TIA Act Annual Report.
[74] Corrections refer to Table 38, page 68, 2020-21 TIA Act Annual Report.
[75] Corrections refer to Table 41, page 72, 2020-21 TIA Act Annual Report.
[76] Corrections refer to Table 42, page 73, 2020-21 TIA Act Annual Report.

QLD Police 2020-21:

QLD Police identified corrections regarding the number of authorisations for existing information and retained data for the 2020-21 Annual Report. The below details both the original figures provided for the 2020-21 Annual Report and the amended figures as identified and corrected.

Number of authorisations made by an enforcement agency for access to existing information or documents for the criminal law – paragraph 186(1)(a)[77]

Agency	Authorisations	
	20/21 original	20/21 updated
QLD Police	25,645	25,764
TOTAL	**312,440**	**313,306[78]**

Number of authorisations made for access to existing information or documents for the location of missing persons – paragraphs 186(1)(aa)[79]

Agency	Authorisations	
	20/21 original	20/21 updated
QLD Police	256	260
TOTAL	**3,490**	**3,513[80]**

Offences for which authorisations were made under section 178 to access existing data to enforce the criminal law – paragraph 186(1)(e)[81]

Categories of offences	QLD 2020-21 Original	QLD 2020-21 Updated
Abduction	2,239	2,251
Acts – injury	16	28
Cybercrime	984	987
Fraud	654	656
Homicide	1,811	1,824
Illicit drug offences	4,251	4,290
Loss of life	564	565
Miscellaneous	6,345	6,348
Justice procedures	-	1
Organised offences	19	20
Weapons	40	41
Property damage	108	113

[77] Corrections refer to Table 30, pages 55-56, 2020-21 TIA Act Annual Report.
[78] This figure includes updates from AFP and NSW Police which are identified in this Appendix.
[79] Corrections refer to Table 31, page 56, 2020-21 TIA Act Annual Report.
[80] This figure includes updates from the AFP which are identified in this Appendix.
[81] Corrections refer to Table 34, page 60-61, 2020-21 TIA Act Annual Report.

Categories of offences	QLD 2020-21 Original	QLD 2020-21 Updated
Robbery	1,211	1,217
Unlawful entry	1,423	1,425
TOTAL	**25,419**	**25,520**

Periods for which retained data was held by carrier before authorised disclosure - paragraph 186(1)(f)[82]

QLD 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
20/21 Original	21,046	1,472	984	625	494	282	246	165	591	**25,905**
20/21 Updated	21,156	1,477	986	625	497	283	246	166	592	**26,028**

Types of retained data disclosed in authorisations – paragraph 186(1)(g) and 186(1)(h)[83]

QLD Police	Item 1: subscriber data	Items 2 – 6: traffic data
20/21 Original	18,570	6,078
20/21 Updated	18,686	6,085

SA Police 2019-21:

SA Police identified corrections regarding the number of domestic preservation notices and convictions in which lawfully intercepted information was given in evidence for the 2019-20 and 2020-21 Annual Reports respectively. The below details both the original figures provided for each Annual Report and the amended figures as identified and corrected.

Domestic preservation notices – subsection 161A(1)[84]

Agency	Domestic preservation notices issued		Domestic preservation revocation notices issued	
	19/20 Original	19/20 Updated	19/20 Original	19/20 Updated
SA Police	120	117	84	76
TOTAL	**2,496**	**2,493**	**811**	**803**

[82] Corrections refer to Table 37, page 67, 2020-21 TIA Act Annual Report.
[83] Correction refers to Table 38, page 68, 2020-21 TIA Act Annual Report.
[84] Corrections refer to Table 26, page 51, 2019-20 TIA Act Annual Report.

Convictions per offence category in which lawfully intercepted information was given in evidence – paragraphs 102(1)(b)-(c) and 102(2)(b)-(c)[85]

Category	SA Police 20/21 Original	SA Police 20/21 Updated
Money laundering	1	**-**
Murder	5	**5**
Serious drug offences and/or trafficking	35	**-**
TOTAL	**41**	**5**

[85] Corrections refer to Table 8, page 19, 2020-21 TIA Act Annual Report.

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