Australian Government
Attorney-General's Department

2022–23 Annual Report under the *Telecommunications (Interception and Access) Act 1979* and Part 15 of the *Telecommunications Act 1997*

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

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

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

Contents

Abbreviations

Abbreviation	Term
AAT	Administrative Appeals Tribunal
ACLEI	Australian Commission for Law Enforcement Integrity
ACCC	Australian Competition and Consumer Commission
ACIC	Australian Criminal Intelligence Commission
AFP	Australian Federal Police
ASIO	Australian Secret Intelligence Organisation
ASIS	Australian Secret Intelligence Service
ASIC	Australian Securities and Investments Commission
ASD	Australian Signals Directorate
AGD	Attorney-General's Department
Ombudsman	Commonwealth Ombudsman
CS NSW	Corrective Services New South Wales
CCC (WA)	Corruption and Crime Commission (Western Australia)
Home Affairs	Department of Home Affairs
IBAC	Independent Broad-based Anti-corruption Commission (Victoria)
ICAC (NSW)	Independent Commission Against Corruption (New South Wales)
ICAC (SA)	Independent Commissioner Against Corruption (South Australia)
IGIS	Inspector-General of Intelligence and Security
IPO	International Production Order
JIW	Journalist Information Warrant
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
PIA	Public Interest Advocate
QLD CCC	Queensland Corruption and Crime Commission
QLD Police	Queensland Police Service
SA Police	South Australia Police

Abbreviation	Term
TAS Police	Tasmania Police
TAN	Technical Assistance Notice
TAR	Technical Assistance Request
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

- There were 3,210 interception warrants that were issued to 15 interception agencies. This was an increase of 3 on the 3,207 issued in 2021–22.
- There were 28 applications for interception warrants that were refused. This increased by 22 compared to 2021–22.
- The majority of serious offences that were specified in interception warrants issued were serious drug offences and/or trafficking (1,339 times), followed by loss of life or personal injury (579 times) and murder (565 times).
- Information obtained under interception warrants was used in 2,501 arrests, 2,275 prosecutions and 1,623 convictions.
- There were 795 stored communications warrants that were issued to 10 criminal law-enforcement agencies. This is a decrease of 12 on the 807 issued in 2021–22.
- There were 2 applications for stored communications warrants that were refused. This was an increase of one from 2021–22.
- Information obtained under stored communications warrants was used in 466 arrests, 156 proceedings, and 164 convictions.
- There were 334,237 authorisations made by 21 enforcement agencies for the disclosure of existing telecommunications data. This is an increase of 21,705 authorisations from the 312,532 authorisations made in 2021–22.[1] Of these, 326,771 were made to enforce the criminal law.
- Authorisations for existing telecommunications data covered a range of crimes, including 63,904 authorisations for illicit drug offences, 34,234 authorisations for unlawful entry and 32,805 authorisations for homicide.
- There were 44,479 authorisations made by 20 criminal law-enforcement agencies for disclosure of prospective telecommunications data. This is an increase of 6,382 on the 38,097 authorisations made in 2021–22.
- No journalist information warrants were issued to enforcement agencies in 2022–23, consistent with 2021–22.
- There were 66 technical assistance requests given to designated communications providers by 5 interception agencies. This is an increase of 36 from 2021–22.
- No technical assistance notices or technical capability notices were given in this reporting period.

[1] This includes adjustments made to the 2021–22 Annual Report (see Appendix D).

Chapter 1: Introduction

The 2022–23 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 2022 and 30 June 2023.

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 communications 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 communications 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. Telecommunications data is information about a communication (such as the phone numbers of the people who called each other, how long they spoke to each other, the email address from which a message was sent and the time the message was sent) or the telecommunications service to which a person has subscribed but not the content of the communication.

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, and only criminal law-enforcement agencies can access prospective telecommunications data to assist in the investigation of offences punishable by at least three years imprisonment.[2] 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.

Criminal law-enforcement agencies may authorise access to telecommunications data. The Attorney-General may also declare additional agencies in limited circumstances for a period of 40 sitting days of Parliament. In the 2022–23 reporting period, the New South Wales Department of Communities and Justice was declared as an enforcement agency. However, this declaration only applies to that part of New South Wales Department of Communities and Justice known as Corrective Services NSW (CS NSW).

[2] 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.

Chapter 2: Telecommunications interception

The interception of communications is regulated by Chapter 2 of the TIA Act. The function of section 7 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 warrant to authorise the interception of a particular telephone number, or a warrant to authorise the interception of multiple services that relate to a named person). During the reporting period, interception warrants were available to 17 Commonwealth, state and territory agencies.

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 7 years imprisonment. There are exceptions to this threshold. Interception warrants may be available for offences with a penalty of less than 7 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 communications is critical to enable the collection of evidence and its availability may be key to resolving an investigation.

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 **Tables 1, 1A, 1B and 1C**. Consistent with previous years, in 2022–23 the majority of warrants obtained were to assist with investigations into serious drug offences and/or trafficking (1,339 warrants). Murder was specified in 565 warrants and 579 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**.

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	Commonwealth agencies	State and Territory Police	State and Territory Integrity Agencies	TOTAL
Administration of justice / government offences	14	2	-	**16**
Assisting person to escape or dispose of proceeds	-	5	2	**7**
Bribery, corruption and dishonesty offences	10	24	37	**71**
Child abuse offences	1	22	-	**23**
Conspire/aid/abet serious offence	1	14	-	**15**
Cybercrime offences	2	-	-	**2**
Espionage and foreign interference	39	2	-	**41**
Kidnapping	1	99	-	**100**
Loss of life or personal injury	16	563	-	**579**
Money laundering	123	20	20	**163**
Murder	51	514	-	**565**
Offences involving planning and organisation	7	156	-	**163**
Organised offences and/or criminal organisations	15	64	3	**82**
People smuggling and related	7	-	-	**7**

Categories of offences	Commonwealth agencies	State and Territory Police	State and Territory Integrity Agencies	TOTAL
Serious damage to property and/or serious arson	1	64	-	**65**
Serious drug offences and/or trafficking	339	977	23	**1,339**
Serious fraud	19	61	1	**81**
Serious loss of revenue	-	2	-	**2**
Special ACC investigations	14	-	-	**14**
Telecommunications offences	-	6	-	**6**
Terrorism offences	83	2	-	**85**
TOTAL	**743**	**2,597**	**86**	**3,426**

Table 1A: Commonwealth agencies – 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	ACLEI	ACIC	AFP	TOTAL
Administration of justice / government offences	8	-	6	**14**
Bribery, corruption and dishonesty offences	8	-	2	**10**
Child abuse offences	-	-	1	**1**
Conspire/aid/abet serious offence	-	-	1	**1**
Cybercrime offences	1	-	1	**2**
Espionage and foreign interference	6	-	33	**39**

Categories of offences	ACLEI	ACIC	AFP	TOTAL
Kidnapping	-	-	1	**1**
Loss of life or personal injury	-	-	16	**16**
Money laundering	2	12	109	**123**
Murder	-	-	51	**51**
Offences involving planning and organisation	-	-	7	**7**
Organised offences and/or criminal organisations	-	-	15	**15**
People smuggling and related	-	-	7	**7**
Serious damage to property and/or serious arson	-	-	1	**1**
Serious drug offences and/or trafficking	2	20	317	**339**
Serious fraud	-	1	18	**19**
Special ACC investigations	-	14	-	**14**
Terrorism offences	-	-	83	**83**
TOTAL	**27**	**47**	**669**	**743**

Table 1B: State and Territory Police – 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	NSW Police	NT Police	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Administration of justice / government offences	2	-	-	-	-	-	-	**2**

Categories of offences	NSW Police	NT Police	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Assisting person to escape or dispose of proceeds	2	-	1	2	-	-	-	**5**
Bribery, corruption and dishonesty offences	13	5	-	-	-	-	6	**24**
Child abuse offences	14	-	-	-	-	4	4	**22**
Conspire/aid/abet serious offence	10	-	-	-	-	4	-	**14**
Espionage and foreign interference	2	-	-	-	-	-	-	**2**
Kidnapping	98	1	-	-	-	-	-	**99**
Loss of life or personal injury	404	3	63	-	-	41	52	**563**
Money laundering	10	-	-	-	-	2	8	**20**
Murder	408	10	3	9	2	40	42	**514**
Offences involving planning and organisation	111	-	-	-	-	-	45	**156**
Organised offences and/or criminal organisations	64	-	-	-	-	-	-	**64**
Serious damage to property and/or serious arson	48	2	6	-	-	-	8	**64**
Serious drug offences and/or trafficking	613	6	166	11	2	54	125	**977**
Serious fraud	51	-	7	-	-	1	2	**61**
Serious loss of revenue	1	-	-	-	-	1	-	**2**

Categories of offences	NSW Police	NT Police	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Telecommunications offences	6	-	-	-	-	-	-	**6**
Terrorism offences	2	-	-	-	-	-	-	**2**
TOTAL	**1,859**	**27**	**246**	**22**	**4**	**147**	**292**	**2,597**

Table 1C: State and Territory Integrity Agencies – 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	CCC (WA)	IBAC	LECC	NSW CC	QLD CCC	TOTAL
Assisting person to escape or dispose of proceeds	-	-	-	2	-	**2**
Bribery, corruption and dishonesty offences	10	13	14	-	-	**37**
Money laundering	2	-	2	4	12	**20**
Organised offences and/or criminal organisations	-	-	-	3	-	**3**
Serious drug offences and/or trafficking	-	-	-	14	9	**23**
Serious fraud	-	-	-	1	-	**1**
TOTAL	**12**	**13**	**16**	**24**	**21**	**86**

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), or
- 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 2023, there were 98 issuing authorities for interception warrants.

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

Issuing authority	Number eligible
Federal Court judges	24
Federal Circuit and Family Court judges	39
Nominated AAT members	35
TOTAL	**98**

Issuing of interception warrants

Table 3 states which issuing authorities considered applications for warrants made by each interception agency during 2022–23. In 2022–23, nominated AAT members considered 82 per cent 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[3]

Agency	Issuing authority			
	Federal Court judges	Federal Circuit and Family Court judges	Nominated AAT members	TOTAL
ACLEI	-	1	7	**8**
ACIC	-	2	25	**27**
AFP	1	81	436	**518**
CCC (WA)	-	12	-	**12**
IBAC	-	-	13	**13**
ICAC (SA)	-	-	-	**-**
LECC	-	-	16	**16**
NSW CC	-	-	18	**18**
NSW Police	-	67	1,809	**1,876**

[3] The telephone and renewal applications made for interception warrants are a subset of the total warrant applications made for each agency.

Agency	Issuing authority			
	Federal Court judges	Federal Circuit and Family Court judges	Nominated AAT members	TOTAL
NT Police	-	21	3	**24**
QLD CCC	-	4	8	**12**
QLD Police	-	185	62	**247**
SA Police	-	-	22	**22**
TAS Police	-	-	5	**5**
VIC Police	-	-	145	**145**
WA Police	-	211	84	**295**
TOTAL	**1**	**584**	**2,653**	**3,238**

Applications for interception warrants

Paragraphs 100(1)(a)-(c) and 100(2)(a)-(c) of the TIA Act provide that this report sets 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 2022–23, agencies were issued 3,210 interception warrants, being an increase of 3 from 2021–22, where 3,207 interception warrants were issued. In 2022–23, 618 renewals of interception warrants were issued. This was an increase of 26 renewals of interception warrants from the 592 issued in the previous reporting period. There was an increase in the number of telephone applications from 10 to 22 compared to the 2021–22 reporting period.

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

Agency	Relevant statistics	Applications for warrants		Telephone applications for warrants		Renewal applications	
		21/22	22/23	21/22	22/23	21/22	22/23
ACLEI	Made	20	8	-	-	7	1
	Refused	-	-	-	-	-	-
	Issued	20	8	-	-	7	1
ACIC	Made	52	27	-	-	6	-
	Refused	-	-	-	-	-	-
	Issued	52	27	-	-	6	-
AFP	Made	475	518	-	-	126	167
	Refused	3	1	-	-	-	-
	Issued	472	517	-	-	126	167
CCC (WA)	Made	23	12	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	23	12	-	-	-	-
IBAC	Made	10	13	-	-	2	3
	Refused	-	2	-	-	-	-
	Issued	10	11	-	-	2	3
ICAC (SA)	Made	2	-	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	2	-	-	-	-	-
LECC	Made	17	16	-	-	5	12
	Refused	-	-	-	-	-	-
	Issued	17	16	-	-	5	12

[4] 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	
		21/22	22/23	21/22	22/23	21/22	22/23
NSW CCC	Made	59	18	-	-	26	3
	Refused	-	-	-	-	-	-
	Issued	59	18	-	-	26	3
NSW Police	Made	1,804	1,876	10	22	326	363
	Refused	1	17	-	-	-	2
	Issued	1,803	1,859	10	22	326	361
NT Police	Made	35	24	-	-	5	1
	Refused	-	-	-	-	-	-
	Issued	35	24	-	-	5	1
QLD CCC	Made	20	12	-	-	10	-
	Refused	-	-	-	-	-	-
	Issued	20	12	-	-	10	-
QLD Police	Made	236	247	-	-	40	43
	Refused	-	1	-	-	-	1
	Issued	236	246	-	-	40	42
SA Police	Made	22	22	-	-	4	2
	Refused	-	-	-	-	-	-
	Issued	22	22	-	-	4	2
TAS Police	Made	12	5	-	-	1	-
	Refused	-	1	-	-	-	-
	Issued	12	4	-	-	1	-
VIC Police	Made	127	145	-	-	15	9
	Refused	-	3	-	-	-	-
	Issued	127	142	-	-	15	9
WA Police	Made	299	295	-	-	19	17
	Refused	2	3	-	-	-	-
	Issued	297	292	-	-	19	17

Agency	Relevant statistics	Applications for warrants		Telephone applications for warrants		Renewal applications	
		21/22	22/23	21/22	22/23	21/22	22/23
TOTAL	Made	3,213	3,238	10	22	592	621
	Refused	6	28	-	-	-	3
	Issued	3,207	3,210	10	22	592	618

Warrants that authorise entry onto 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 onto premises.

In 2022–23, no warrants were issued authorising entry on premises. This is a decrease from 2021–22, where one warrant authorising entry on premises was 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	
	21/22	22/23
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 reporting period specified conditions or restrictions relating to interceptions under the warrants.

This information is presented in **Table 6**. In 2022–23, 58 interception warrants were issued with a condition or restriction. This is a decrease of 49 compared to the 107 issued in 2021–22.

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	
	21/22	22/23
ACLEI	2	-
AFP	1	2
LECC	2	1
NSW Police	99	55
QLD CCC	3	-
TOTAL	**107**	**58**

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 removed 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 prescribed offences proceedings by way of prosecutions which ended during that year. This means 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 where convictions were recorded.

This information is provided in **Tables 7, 8 and 9**. In 2022–23, there were 2,501 arrests made as a result of lawfully intercepted information. There were also 2,275 prosecutions and 1,623 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	21/22		22/23	
	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
ACLEI	2	2	-	2
ACIC	-	20	-	-
AFP	125	7	63	50
ICAC (SA)	2	1	-	-
NSW CC	-	57	-	38
NSW Police	1,471	7	1,802	16

Agency	21/22		22/23	
	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
NT Police	22	-	20	-
QLD CCC	-	3	-	1
QLD Police	227	-	201	-
SA Police	27	-	19	2
TAS Police	3	3	1	1
VIC Police	325	48	164	38
WA Police	310	218	231	154
TOTAL	**2,514**	**366**	**2,501**	**302**

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	AFP	ICAC (NSW)	LECC	NSW CC	NSW Police	QLD CCC	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Administration of justice / government offence	1	3	-	-	-	1	-	-	-	-	-	-	**5**
Ancillary offences	-	-	-	-	-	-	-	-	-	-	2	-	**2**
Assisting to escape or dispose of proceeds	-	-	-	-	-	2	-	-	-	-	-	-	**2**
Bribery or corruption	1	-	-	-	-	3	3	-	-	-	-	-	**7**
Cartel offences	-	2	-	-	-	-	-	-	-	-	-	-	**2**
Child abuse offences	-	-	-	2	-	2	-	-	-	-	-	8	**12**
Conspire/aid/abet serious offence	-	3	-	-	-	10	-	-	2	-	4	-	**19**
Cybercrime offences	-	2	-	-	-	-	-	-	-	-	-	-	**2**
Kidnapping	-	-	-	-	-	6	-	-	-	-	-	-	**6**
Loss of life	-	-	-	-	-	1	-	-	-	-	5	-	**6**
Money laundering	-	18	-	-	-	28	-	1	-	-	8	42	**97**
Murder	-	1	-	-	-	31	-	-	-	-	6	8	**46**

Category	ACLEI	AFP	ICAC (NSW)	LECC	NSW CC	NSW Police	QLD CCC	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Offences involving planning and organisation	-	3	-	-	-	42	-	-	-	-	12	79	**136**
Organised crime	-	4	-	-	-	25	-	-	-	-	-	-	**29**
Other offences punishable by 3 years to life	-	4	2	-	-	216	1	5	-	-	47	-	**275**
Serious arson	-	-	-	-	-	5	-	-	-	-	1	3	**9**
Serious damage to property	-	-	-	-	-	48	-	-	-	-	-	10	**58**
Serious drug offences and/or trafficking	-	94	-	-	1	287	3	3	3	1	59	1,010	**1,461**
Serious fraud	-	5	-	-	-	5	1	-	-	-	7	8	**26**
Serious loss of revenue	-	1	-	-	-	20	-	-	-	-	-	-	**21**
Serious personal injury	-	-	-	-	-	18	-	-	-	-	15	12	**45**
Terrorism offences	-	9	-	-	-	-	-	-	-	-	-	-	**9**
TOTAL	**2**	**149**	**2**	**2**	**1**	**750**	**8**	**9**	**5**	**1**	**166**	**1,180**	**2,275**

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	ACLEI	AFP	ICAC (NSW)	LECC	NSW CC	NSW Police	QLD CCC	QLD Police	SA Police	VIC Police	WA Police	TOTAL
Administration of justice / government offence	1	1	-	-	-	1	-	-	-	-	-	**3**
Ancillary offences	-	-	-	-	-	-	-	-	-	2	-	**2**
Assisting person to escape or dispose of proceeds	-	-	-	-	-	2	-	-	-	-	-	**2**
Bribery or corruption	1	-	-	-	-	2	1	-	-	-	-	**4**
Child abuse offences	-	-	-	1	-	2	-	-	-	-	4	**7**
Conspire/aid/abet serious offence	-	1	-	-	-	9	-	-	-	3	-	**13**
Kidnapping	-	-	-	-	-	5	-	-	-	-	-	**5**
Loss of life	-	-	-	-	-	1	-	-	-	5	-	**6**
Money laundering	-	7	-	-	-	26	-	1	-	8	21	**63**
Murder	-	-	-	-	-	24	-	-	-	5	3	**32**

Category	ACLEI	AFP	ICAC (NSW)	LECC	NSW CC	NSW Police	QLD CCC	QLD Police	SA Police	VIC Police	WA Police	TOTAL
Offences involving planning and organisation	-	-	-	-	-	40	-	-	-	12	36	**88**
Organised crime	-	-	-	-	-	4	-	-	-	-	-	**4**
Other offences punishable by 3 years to life	-	1	2	-	-	180	1	5	-	46	-	**235**
Serious arson	-	-	-	-	-	5	-	-	-	1	1	**7**
Serious damage to property	-	-	-	-	-	48	-	-	-	-	3	**51**
Serious drug offences and/or trafficking	-	50	-	-	1	261	3	3	2	57	650	**1,027**
Serious fraud	-	2	-	-	-	5	1	-	-	6	4	**18**
Serious loss of revenue	-	-	-	-	-	20	-	-	-	-	-	**20**
Serious personal injury	-	-	-	-	-	18	-	-	-	12	5	**35**
Terrorism offences	-	1	-	-	-	-	-	-	-	-	-	**1**
TOTAL	**2**	**63**	**2**	**1**	**1**	**653**	**6**	**9**	**2**	**157**	**727**	**1,623**

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 less intrusive means 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 reporting period specified conditions or restrictions relating to interceptions under the warrants.

This information is presented in **Tables 10 and 11**. In 2022–23, 488 named person warrants were issued. This is an increase of 30 from 2021–22, in which 458 named person warrants were issued. There was also an increase of 22 renewal applications from 122 in 2021–22 to 144 in 2022–23.

Table 10: Applications, telephone applications, and renewal applications for named person warrants – paragraphs 100(1)(ea) and 100(2)(ea)[5]

Agency	Relevant statistics	Applications		Telephone applications		Renewal applications	
		21/22	22/23	21/22	22/23	21/22	22/23
ACLEI	Made	-	2	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	-	2	-	-	-	-
ACIC	Made	23	9	-	-	2	-
	Refused	-	-	-	-	-	-
	Issued	23	9	-	-	2	-
AFP	Made	149	237	-	-	42	79
	Refused	-	-	-	-	-	-
	Issued	149	237	-	-	42	79
CCC (WA)	Made	4	4	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	4	4	-	-	-	-
IBAC	Made	2	-	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	2	-	-	-	-	-
LECC	Made	13	16	-	-	5	12
	Refused	-	-	-	-	-	-
	Issued	13	16	-	-	5	12
NSW CC	Made	26	4	-	-	17	1
	Refused	-	-	-	-	-	-
	Issued	26	4	-	-	17	1

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

Agency	Relevant statistics	Applications		Telephone applications		Renewal applications	
		21/22	22/23	21/22	22/23	21/22	22/23
NSW Police	Made	133	127	1	-	37	50
	Refused	-	-	-	-	-	-
	Issued	133	127	1	-	37	50
NT Police	Made	5	2	-	-	2	-
	Refused	-	-	-	-	-	-
	Issued	5	2	-	-	2	-
QLD CCC	Made	5	-	-	-	2	-
	Refused	-	-	-	-	-	-
	Issued	5	-	-	-	2	-
QLD Police	Made	28	13	-	-	7	2
	Refused	-	1	-	-	-	1
	Issued	28	12	-	-	7	1
SA Police	Made	7	3	-	-	2	1
	Refused	-	-	-	-	-	-
	Issued	7	3	-	-	2	1
VIC Police	Made	22	32	-	-	4	-
	Refused	-	-	-	-	-	-
	Issued	22	32	-	-	4	-
WA Police	Made	41	40	-	-	2	-
	Refused	-	-	-	-	-	-
	Issued	41	40	-	-	2	-
TOTAL	**Made**	**458**	**489**	**1**	**-**	**122**	**145**
	Refused	**0**	**1**	**0**	**-**	**0**	**1**
	Issued	**458**	**488**	**1**	**-**	**122**	**144**

In 2022–23, 5 named person warrants were issued with a condition or restriction. This is the same as in 2021–22.

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	
	21/22	22/23
AFP	-	1
LECC	2	1
NSW Police	2	3
QLD CCC	1	-
TOTAL	**5**	**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 2022–23 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	
	21/22	22/23	21/22	22/23	21/22	22/23	21/22	22/23
ACLEI	-	-	-	2	-	-	-	-
ACIC	11	6	10	3	-	-	-	-
AFP	34	70	94	153	7	9	-	3
CCC (WA)	3	2	1	2	-	-	-	-
IBAC	-	-	2	-	-	-	-	-
LECC	-	3	13	13	-	-	-	-
NSW CC	7	1	19	3	-	-	-	-
NSW Police	51	49	78	53	6	2	-	-

Agency	Named person warrants by number of services intercepted							
	1 service only		2-5 services		6-10 services		10+ services	
	21/22	22/23	21/22	22/23	21/22	22/23	21/22	22/23
NT Police	-	-	5	2	-	-	-	-
QLD CCC	2	-	2	-	1	-	-	-
QLD Police	10	1	14	10	4	1	-	-
SA Police	1	-	6	3	-	-	-	-
TAS Police	-	-	-	-	-	-	-	-
VIC Police	6	7	15	10	1	-	-	-
WA Police	7	20	30	20	4	-	-	-
TOTAL	**132**	**159**	**289**	**274**	**23**	**12**	**-**	**3**

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:

- services intercepted under service based named person warrants
- services intercepted under device based named person warrants, and
- telecommunications devices intercepted under device-based named person warrants.

Definitions

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.

A **'telecommunications device'** is also 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.

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	
	21/22	22/23
ACLEI	-	4
ACIC	36	17
AFP	335	524
CCC (WA)	4	8
IBAC	5	-
LECC	35	39
NSW CC	26	12
NSW Police	138	237
NT Police	15	8
QLD CCC	12	-
QLD Police	81	37
SA Police	16	12
TAS Police	-	-
VIC Police	52	36
WA Police	106	69
TOTAL	**861**	**1,003**

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	
	21/22	22/23	21/22	22/23
AFP	21	59	30	-
NSW Police	18	17	39	22
NT Police	2	-	-	-
VIC Police	-	15	-	-
WA Police	2	-	-	-
TOTAL	**43**	**91**	**69**	**22**

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 by 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 2022–23, 118 B-Party warrants were issued to interception agencies. This represents an increase of 61 from the 57 B-Party warrants issued in 2021–22. In 2022–23, one B-Party warrant was issued with conditions or restrictions. This is a decrease of 3 from the 4 issued in 2021–22.

Table 15: Applications for B-Party warrants, telephone applications and renewal applications for B-Party warrants – paragraphs 100(1)(ed) and 100(2)(ed)[6]

Agency	Relevant statistics	Applications for B-Party warrants		Telephone applications for B-Party warrants		Renewal applications for B-Party warrants	
		21/22	22/23	21/22	22/23	21/22	22/23
ACIC	Made	2	-	-	-	1	-
	Refused	-	-	-	-	-	-
	Issued	2	-	-	-	1	-
AFP	Made	11	26	-	-	3	10
	Refused	1	-	-	-	-	-
	Issued	10	26	-	-	3	10
NSW Police	Made	43	92	2	7	2	5
	Refused	-	-	-	-	-	-
	Issued	43	92	2	7	2	5
QLD Police	Made	1	-	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	1	-	-	-	-	-
VIC Police	Made	1	-	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	1	-	-	-	-	-
TOTAL	**Made**	**58**	**118**	**2**	**7**	**6**	**15**
	Refused	**1**	**-**	**-**	**-**	**-**	**-**
	Issued	**57**	**118**	**2**	**7**	**6**	**15**

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

Table 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	
	21/22	22/23
AFP	1	-
NSW Police	3	1
TOTAL	**4**	**1**

In 2022–23, no B-Party warrants were issued authorising entry onto premises. This is the same as the previous year.

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. This information is presented in **Table 17**.

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)[7]	Average period specified in warrants (days)	Average period warrants in force (days)[8]
ACLEI	90	78	90	90
ACIC	85	73	-	-
AFP	84	63	86	75
CCC (WA)	90	74	-	-
IBAC	64	35	65	56
LECC	90	90	89	77
NSW CC	89	77	90	81
NSW Police	74	52	79	65
NT Police	90	59	90	90
QLD CCC	90	65	-	-
QLD Police	78	63	81	62
SA Police	84	61	90	43
TAS Police	90	61	-	-
VIC Police	85	57	87	52
WA Police	89	40	90	81
AVERAGE	**79**	**54**	**81**	**75**

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

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. This information is presented in **Table 18**.

Table 18: Duration of original and renewal B-Party warrants – paragraphs 101(1)(da) and 101(2)(da)

Agency	Duration of original B-Party warrants		Duration of renewal telecommunications B-Party warrants	
	Average period specified in warrants (days)	Average period warrants in force (days)[9]	Average period specified in warrants (days)	Average period warrants in force (days)[10]
AFP	45	37	45	44
NSW Police	35	25	42	-
AVERAGE	**37**	**27**	**44**	**44**

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 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**.

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

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

Agency	90 days		150 days		180 days	
	21/22	22/23	21/22	22/23	21/22	22/23
ACLEI	-	1	-	-	3	-
ACIC	4	-	-	1	-	-
AFP	26	24	28	39	34	47
IBAC	-	3	2	-	-	-
LECC	2	-	1	-	-	3
NSW CC	2	-	1	-	6	3
NSW Police	118	85	53	57	64	52
NT Police	-	-	-	1	1	-
QLD CCC	4	-	-	-	-	-
QLD Police	9	19	7	15	8	3
SA Police	2	2	-	-	1	-
VIC Police	4	2	6	4	1	2
WA Police	15	7	4	10	1	-
TOTAL	**186**	**143**	**102**	**127**	**119**	**110**

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 warrant' 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 2022–23, 69% of total warrants were eligible warrants.

Table 20: Percentage of eligible warrants – subsections 102(3) and 102(4)[11]

Agency	Number of eligible warrants	Total number of warrants in force	%
ACLEI	3	10	30%
ACIC	14	31	45%
AFP	277	595	47%
CCC (WA)	0	16	0%
IBAC	11	11	100%
LECC	17	19	89%
NSW CC	8	25	32%
NSW Police	1,525	2,028	75%
NT Police	6	35	17%
QLD CCC	6	12	50%
QLD Police	272	291	93%
SA Police	21	26	81%
TAS Police	1	4	25%
VIC Police	53	156	34%
WA Police	238	317	75%
TOTAL	**2,452**	**3,576**	**69%**

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).

[11] 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.

Table 21: Number of occasions on which an officer or staff member of an agency intercepted a communication in reliance on subsection 7(4) or 7(5) – section 102A

Agency	21/22	22/23
AFP	-	1
TOTAL	**-**	**1**

In 2022–23, the AFP intercepted a communication without a warrant on one occasion. The AFP advised this occurred with the consent of the person to whom the communication was directed, where there were reasonable grounds for believing that that person is likely to receive a communication from another person who has threated to kill or seriously injure another person or to cause serious damage to property.

Subsection 7(6) requires that as soon as practicable after the interception of a communication in reliance on subsection 7(4) or 7(5), an officer of the agency shall cause an application for an interception warrant to be made in relation to the matter.

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 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 2022–23, there were 2 occasions in which lawfully intercepted information or interception warrant information was provided to a foreign country under subsection 13A(1) of the *Mutual Assistance in Criminal Matters Act 1987*. This is an increase of 2 from 2021–22.

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 22: Interceptions carried out on behalf of other agencies – paragraph 103(ac)

Interception carried out by:	Interception carried out on behalf of	Number of interceptions
VIC Police	Queensland CCC	12
VIC Police	Tasmania Police	4

Telecommunications interception expenditure

Table 23 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 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 23: 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
ACLEI	$90,040	$11,255
ACIC	$6,245,446	$231,313
AFP	$12,307,653	$23,806
CCC (WA)	$577,697	$48,141
IBAC	$859,496	$78,136
ICAC (NSW)	$488,732	-
ICAC (SA)	$87,767	-
LECC	$1,338,076	$83,630
NSW CC	$1,965,541	$109,197
NSW Police	$22,297,996	$11,995
NT Police	$1,733,570	$72,232
QLD CCC	$1,329,337	$110,778
QLD Police	$7,909,045	$32,151
SA Police	$4,146,158	$188,462
TAS Police	$1,135,333	$283,833
VIC Police	$462,570	$3,258
WA Police	$4,401,416	$15,073
TOTAL / AVERAGE	**$67,375,873**	**$20,962**

The breakdown of the total recurrent costs of interception over the reporting period is provided in **Table 24**. 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 24: Recurrent interception costs per agency

Agency	Salaries	Administrative support	Capital expenditure	Interception costs	Total ($)
ACLEI	$88,000	-	-	$2,040	**$90,040**
ACIC	$4,251,252	$368,172	$115,905	$1,510,117	**$6,245,446**
AFP	$7,337,968	$458,352	-	$4,511,333	**$12,307,653**
CCC (WA)	$311,197	$560	$207,978	$57,962	**$577,697**
IBAC	$607,990	$21,210	$60,761	$169,535	**$859,496**
ICAC (NSW)	$239,557	-	-	$249,175	**$488,732**
ICAC (SA)	-	-	-	$87,767	**$87,767**
LECC	$740,444	$883	$298,000	$298,749	**$1,338,076**
NSW CC	$1,389,919	$9,890	$400,000	$165,732	**$1,965,541**
NSW Police	$7,300,931	$161,075	$11,438,357	$3,397,633	**$22,297,996**
NT Police	$633,373	$121,395	$970,167	$8,635	**$1,733,570**
QLD CCC	$885,157	$222,680	-	$221,500	**$1,329,337**
QLD Police	$5,265,496	$931,341	$24,090	$1,688,118	**$7,909,045**
SA Police	$2,378,695	$277,833	$542,909	$946,721	**$4,146,158**
TAS Police	$950,082	$18,784	$12,946	$153,521	**$1,135,333**
VIC Police	$308,801	$33,647	$26,803	$93,319	**$462,570**
WA Police	$3,840,200	-	$50,000	$511,216	**$4,401,416**
TOTAL	**$36,529,062**	**$2,625,822**	**$14,147,916**	**$14,073,073**	**$67,375,873**

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 provides 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 25** sets out the number of premises that have been declared in 2022–23 under the TIA Act to be emergency service facilities. It does not include facilities that were declared in a previous reporting period, unless the declaration instrument was remade in 2022-23.

Table 25: Emergency service facility declaration – paragraph 103(ad)

State	Police	Fire brigade	Ambulance	Despatching
New South Wales	0	0	1	0
Tasmania	1	1	1	2
Western Australia	2	2	2	7
TOTAL	**3**	**3**	**4**	**9**

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 the Attorney-General's Department (AGD) with a copy of each interception warrant
- interception agencies to report to the Attorney-General, within 3 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 3 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 3 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 2022.

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 record of the ACIC, the ACLEI, and the AFP in relation to interception, the relevant state or territory Ombudsman generally undertakes this function for state or 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 related to enforcement agencies (including both Commonwealth and state agencies) access to stored communications and telecommunications data.

Ombudsman – inspection of telecommunications records conducted in 2022–23

Overview

During 2022–23, the Ombudsman conducted 6 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 2022, and consisted of:

- 2 inspections at the AFP
- 2 inspections at the ACIC, and
- 2 inspections at the ACLEI.

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 where appropriate.

Below is a summary of the findings from the 6 inspections the Ombudsman conducted during 2022–23. Where agencies advised of action taken to address the Ombudsman's findings, the Ombudsman will review this action during their 2023–24 inspections.

Sections 79 and 79AA: Destruction of restricted records

Section 79 and 79AA of the TIA Act set out the requirements for destroying restricted records.[12]

Subsection 79(1) of the TIA Act provides that, where the chief officer of the agency is satisfied a restricted record is not likely to be required for a permitted purpose, the chief officer shall cause the restricted record to be destroyed 'forthwith'. 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 Warrants has been inspected by the Attorney-General.[13]

Section 79AA of the TIA Act requires the chief officer to cause destruction of restricted records obtained under a Part 5.3 supervisory order in certain circumstances. The Ombudsman did not make any findings in relation to compliance with section 79AA of the TIA Act from its inspections conducted in 2022–23.

---

[12] 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.
[13] The Secretary of AGD is to cause a General Register of Warrants to be kept in accordance with section 81A of the TIA Act.

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 data, the Ombudsman reported that agencies should have a process to consider whether restricted records are required for a permitted purpose and, if not, destroy the records in line with the TIA Act.

ACIC

In the Ombudsman's 2020–21 annual report to the Attorney-General, the Ombudsman identified that the ACIC did not regularly consider when restricted records should be destroyed and had not set an internal timeframe for when destructions are completed 'forthwith' in accordance with subsection 79(1) of the TIA Act. At the time, the ACIC had not completed destructions in accordance with section 79 of the TIA Act since at least October 2012

In the Ombudsman's 2021–22 annual report, the Ombudsman noted the ACIC had commenced a project to destroy historical telecommunications interception restricted records. The ACIC had audited records for review and was in the process of hiring additional staff to assist in completing the project. However, no destructions were completed within the records period, and the Ombudsman was unable to review any of the ACIC's new or developing processes in action.

During the Ombudsman's first inspection in September 2022, the Ombudsman found that the ACIC had completed its first batch of destructions under the project. However, it did not have documented guidance for managing destructions of restricted records. As a result, the Ombudsman suggested that it would be better practice for the ACIC to draft a practical guidance document that detailed the policies and procedures involved with managing its destruction obligations under section 79 of the TIA Act.

By the Ombudsman's second inspection in March 2023, the ACIC had drafted (but not finalised) standard operating procedures for the destruction of restricted records. The Ombudsman reviewed these during the inspection and suggested that it would be better practice for restricted records to be reviewed at the completion of each investigation (including post any related court proceedings), and for rolling annual reviews of restricted record holdings retained post the investigation, to enable compliance with the destruction requirements of Chapter 2 of the TIA Act. In response, the ACIC advised that it reviews warrant holdings for destruction or retention on a 3 yearly basis, which reflects the ongoing nature of the ACIC's investigations and allows for longer-term prosecutorial opportunities.

The Ombudsman remain concerned about the slow progress of the ACIC's destructions project. At the Ombudsman's inspections in 2023–24 the

Ombudsman will focus on the ACIC's compliance with the destruction requirements of the TIA Act, including progress of the destructions project, with an expectation that the ACIC improves its level of compliance.

ACLEI

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

AFP

The Ombudsman identified one restricted record held by the AFP that was authorised for destruction but had not been destroyed. The destruction of the restricted record was authorised by the chief officer's delegate in July 2022, but had not been destroyed at the time of the Ombudsman's February 2023 inspection due to an administrative error. Upon being informed of this issue, the AFP obtained a new destruction order and destroyed the restricted record in March 2023.

Section 80: Record-keeping in connection with telecommunications interception warrants

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

Based on the Ombudsman's inspections it was satisfied that the ACIC, the ACLEI 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.

ACIC

The Ombudsman assessed the ACIC as compliant with section 81 of the TIA Act.

ACLEI

The Ombudsman assessed the ACLEI as compliant with section 81 of the TIA Act.

AFP

During the Ombudsman's first inspection at the AFP in August 2022, the Ombudsman identified 5 instances where the recording of the use of lawfully intercepted information was not adequate to meet the record-keeping requirements of the TIA Act. This included either providing no documentation to indicate use (or non-use) of lawfully intercepted information or descriptions of use which were too broad to be meaningful.

The Ombudsman suggested that the AFP review the records for the 5 instances and provide a fulsome record of any usage of the lawfully intercepted information. The Ombudsman also suggested it would be better practice for the AFP to consider including an example entry on the usage report template that may assist officers to understand the appropriate level of detail to include in this record. The AFP sought policy advice from AGD regarding the level of detail required in use and communication records and committed to take appropriate action in accordance with that advice.

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.

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

Using lawfully intercepted information and interception warrant information for intelligence purposes

During the Ombudsman's inspection it observed that the ACIC was considering using lawfully intercepted information and interception warrant information for general intelligence purposes.

Whilst the TIA Act permits law enforcement agencies to deal with lawfully intercepted information and warrant information for secondary purposes, these

purposes are limited. The Ombudsman suggested to the ACIC that it would be better practice for them to seek legal advice before it uses lawfully intercepted information or interception warrant information for general intelligence purposes. The ACIC accepted the Ombudsman's better practice suggestion.

Insufficient information provided in affidavits for named person warrants

At the Ombudsman's second inspection of the ACIC in March 2023, the Ombudsman identified 2 named person warrants that relied on the same affidavit that contained insufficient grounds to justify the suspicion that the targets were using, or likely to use, more than one service as required by paragraph 46A(1)(c) of the TIA Act. In these instances, the affidavit referenced the investigator's experience of targets often using more than one service but did not detail the reason for suspecting that the specific target of the named person warrant was using more than one service. While the Ombudsman acknowledged that an investigator's experience adds weight to forming a reasonable suspicion, the Ombudsman considered that experience alone, in the absence of supporting or corroborative information, was insufficient to meet the grounds of 'reasonable suspicion'.

As a result of this finding, the Ombudsman suggested that the ACIC implement controls to ensure that applications for named person warrants detail the reasonable grounds for suspecting that a particular person is using, or is likely to use, more than one telecommunications service. The ACIC's response confirmed that it has controls in place to ensure compliance with this requirement and will review its templates so that it can prevent future non-compliance.

Notifications to the Secretary not sent as soon as practicable

Under subsection 59A(2) of the TIA Act, where a named person warrant is in effect and a service is intercepted under that warrant, the chief officer must cause the Secretary of AGD to be given, as soon as practicable, a description in writing of the service sufficient to identify it.

At the Ombudsman's second inspection of the ACLEI in March 2023, the Ombudsman identified one named person warrant where notifications under subsection 59A(2) of relevant service numbers intercepted under the warrant were not available on the relevant file. The ACLEI acknowledged that the notification step for this warrant had been missed and wrote to the Secretary addressing the oversight during the inspection.

As a result of this finding, the Ombudsman made a suggestion that it would be better practice for the ACLEI to implement appropriate procedural controls and quality assurance practices to support future compliance with subsection 59A(2) of the TIA Act. In its response the ACLEI advised that it had implemented this better practice suggestion by creating and including a notification template in its standard operating procedures. The Ombudsman will monitor this issue at future inspections.

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 for a stored communications warrant to investigate a 'serious contravention' as defined in the TIA Act.

Definition

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.

'Criminal law-enforcement agencies' are set out at section 110A of the TIA Act. These agencies include all interception agencies as well as the Department of Home Affairs (Home Affairs), ASIC and the ACCC.

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

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 3 years, and
- offences punishable by a fine of at least 180 penalty units ($49,500 at the end of the reporting period) for individuals or 900 penalty units ($247,500 at the end the reporting period) if the offence cannot be committed by an individual, such as a corporation.

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

This information is presented in **Table 26**. In 2022–23, 795 stored communications warrants were issued, representing a decrease of 12 from the 807 stored communications warrants issued in 2021–22.

Table 26: 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	
		21/22	22/23	21/22	22/23	21/22	22/23
ACCC	Made	1	-	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	1	-	-	-	-	-
AFP	Made	36	22	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	36	22	-	-	-	-
CCC (WA)	Made	-	1	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	-	1	-	-	-	-
IBAC	Made	8	1	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	8	1	-	-	-	-
NSW CC	Made	2	-	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	2	-	-	-	-	-
NSW Police	Made	406	430	-	1	-	-
	Refused	-	1	-	-	-	-
	Issued	406	429	-	1	-	-

Agency	Relevant statistics	Applications for stored communications warrants		Telephone applications for stored communications warrants		Renewal applications for stored communications warrants	
		21/22	22/23	21/22	22/23	21/22	22/23
NT Police	Made	5	3	-	-	-	-
	Refused	1	-	-	-	-	-
	Issued	4	3	-	-	-	-
QLD Police	Made	98	96	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	98	96	-	-	-	-
SA Police	Made	16	22	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	16	22	-	-	-	-
TAS Police	Made	29	25	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	29	25	-	-	-	-
VIC Police	Made	125	115	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	125	115	-	-	-	-
WA Police	Made	82	82	-	-	-	-
	Refused	-	1	-	-	-	-
	Issued	82	81	-	-	-	-
TOTAL	**Made**	**808**	**797**	**-**	**1**	**-**	**-**
	Refused	**1**	**2**	**-**	**-**	**-**	**-**
	Issued	**807**	**795**	**-**	**1**	**-**	**-**

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 reporting period specified conditions or restrictions relating to access to stored communications under warrants.

This information is presented in **Table 27**. In 2022–23, 497 stored communications warrants were subject to conditions or restrictions, this is an increase of 31 warrants compared to 2021–22.

Table 27: Stored communications warrants subject to conditions or restrictions – paragraph 162(2)(d)

Agency	21/22	22/23
AFP	14	19
NSW CC	1	-
NSW Police	406	429
SA Police	16	22
TAS Police	29	25
VIC Police	-	2
TOTAL	**466**	**497**

Effectiveness of stored communications warrants

Section 163 of the TIA act provides 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. This report must also set out how many proceedings, in which lawfully accessed information was given in evidence, ended during the reporting period.

This information is presented in **Table 28**. In 2022–23, criminal law-enforcement agencies made 466 arrests, conducted 156 proceedings, and obtained 164 convictions involving evidence obtained under stored communications warrants.

Table 28: Arrests, proceedings and convictions made on the basis of lawfully accessed information – paragraphs 163(a)-(b)

Agency	Arrests		Proceedings		Convictions	
	21/22	22/23	21/22	22/23	21/22	22/23
ACIC	-	-	1	-	1	-
AFP	5	16	10	4	11	4
NSW Police	219	335	549	55	332	49
QLD Police	78	56	10	48	10	48
SA Police	-	-	5	4	8	-
TAS Police	1	7	-	4	-	-
VIC Police	54	52	19	41	27	63
TOTAL	**357**	**466**	**594**	**156**	**389**	**164**

Care should be taken in interpreting **Table 28** as an arrest recorded in one reporting period may not result in a prosecution until a later reporting period (if any). 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 3 types of preservation notices:

- *Historic domestic preservation notices* – requires the preservation of all stored communications held by the carrier from the time it receives 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 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 29**. In 2022–23, 1,577 domestic preservation notices were given. This is a decrease of 25 notices on the 1,602 given in 2021–22.

Table 29: Domestic preservation notices – subsection 161A(1)

Agency	Domestic preservation notices issued		Domestic preservation revocation notices issued	
	21/22	22/23	21/22	22/23
ACLEI	2	-	1	-
ACCC	1	-	-	-
AFP	252	141	136	90
CCC (WA)	5	4	-	2
Home Affairs	-	-	-	-
IBAC	8	15	2	5
ICAC (NSW)	-	-	-	-
ICAC (SA)	2	-	2	-
LECC	1	-	1	-
NSW CC	2	-	-	-
NSW Police	599	656	131	131
NT Police	27	48	6	33
QLD CCC	10	12	10	3
QLD Police	261	225	93	63

Agency	Domestic preservation notices issued		Domestic preservation revocation notices issued	
	21/22	22/23	21/22	22/23
SA Police	70	48	52	28
TAS Police	58	69	24	43
VIC Police	150	157	29	21
WA Police	154	202	64	104
TOTAL	**1,602**	**1,577**	**551**	**523**

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 2022–23, no foreign preservation notices or revocation notices were given. This is the same as in 2021–22.

International assistance

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

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

An 'international offence' is:

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

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 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.

In 2022–23, no applications were made for stored communications warrants as a result of an international assistance application. This is the same as in 2021–22.

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 2022–23, 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 2021–22.

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 talk 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, 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 15 March 2023, the New South Wales Department of Communities and Justice was declared an enforcement agency. However, this declaration only applies to that part of New South Wales Department of Communities and Justice known as CS NSW.

Telecommunications data is often the first source of lead information for an investigation, helping to eliminate potential suspects and to support applications for more privacy intrusive investigative tools, including search warrants and interception warrants.

All enforcement agencies can access existing data, whereas 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.

Definitions

‘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 the 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 the officer 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 provide 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 30**. In 2022–23, there were 326,771 authorisations made by agencies under section 178 of the TIA Act. This is an increase of 20,212 from the 306,559 authorisations made in 2021–22.

Table 30: 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	
	21/22	22/23
ACLEI	265	298
ACCC	31[14]	44
ACIC	4,582	4,894
AFP	14,856	14,304
ASIC	455	239
CS NSW	-	2
CCC (WA)	53	109
Home Affairs	3,409	2,465
IBAC	344[15]	286
ICAC (NSW)	201	125
ICAC (SA)	79	111
LECC	517	515
NSW CC	3,007	2,171
NSW Police	105,142[16]	113,078

[14] Correction for 2021–22: ACCC figures relating to authorisations made in relation to the enforcement of the criminal law have been amended due to a reporting error in the 2021–22 Annual Report. As such, the figures have been amended. Appendix D provides both the original figures reported for the 2021–22 period, and the amended figures as identified and amended by ACCC.
[15] Correction for 2021–22: IBAC figures relating to authorisations made in relation to the enforcement of the criminal law have been amended due to a reporting error in the 2021–22 Annual Report. As such, the figures have been amended. Appendix D provides both the original figures reported for the 2021–22 period, and the amended figures as identified and amended by IBAC.
[16] Correction for 2021–22: 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 2021–22 Annual Report. As such, the figures have been amended. Appendix D provides both the original figures reported for the 2021–22 period, and the amended figures as identified and amended by NSW Police.

Agency	Authorisations	
	21/22	22/23
NT Police	2,325	2,158
QLD CCC	595	353
QLD Police	26,051	27,663
SA Police	4,501	7,026
TAS Police	4,821	4,113
VIC Police	108,043	112,749
WA Police	27,282	34,068
TOTAL	**306,559**[17]	**326,771**

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 territory can authorise the disclosure of telecommunications data if the officer 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 reporting period.

This information is presented in **Table 31**. In 2022–23, there were 6,119 authorisations made by agencies under section 178A of the TIA Act. This is an increase of 1,897 from the 4,222 authorisations made in 2021–22.

[17] Correction for 2021–22: ACCC, IBAC and 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 2021–22 Annual Report. As such, the figures have been amended. Appendix D provides both the original figures reported for the 2021–22 period, and the amended figures as identified and amended by these agencies.

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

Agency	Authorisations	
	21/22	22/23
AFP	59	73
NSW Police	2,529[18]	2,709
NT Police	36[19]	36
QLD Police	510	364
SA Police	49	128
TAS Police	83	1,302
VIC Police	779	1,134
WA Police	177	373
TOTAL	**4,222[20]**	**6,119**

[18] Correction for 2021–22: NSW Police figures relating to authorisations for location of missing persons have been amended due to a reporting error in the 2021–22 Annual Report. As such, the figures have been amended. Appendix D provides both the original figures reported for the 2021–22 period, and the amended figures as identified and amended by NSW Police.
[19] Correction for 2021–22: NT Police figures relating to authorisations for location of missing persons have been amended due to a reporting error in the 2021–22 Annual Report. As such, the figures have been amended. Appendix D provides both the original figures reported for the 2021–22 period, and the amended figures as identified and amended by NT Police.
[20] Correction for 2021–22: NSW Police and NT Police figures relating to authorisations for location of missing persons have been amended due to a reporting error in the 2021–22 Annual Report. As such, the figures have been amended. Appendix D provides both the original figures reported for the 2021–22 period, and the amended figures as identified and amended by these agencies.

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 the officer 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 provide that this report must set out the number of authorisations made under section 179 by agencies during the reporting period.

This information is presented in **Table 32**. In 2022–23, there were 1,347 authorisations made by agencies under section 179 of the TIA Act. This is a decrease of 404 from the 1,751 authorisations made in 2021–22.

Table 32: Authorisations made 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	
	21/22	22/23
ACCC	6[21]	-
AFP	4	10
ASIC	51	7
Home Affairs	44	20

[21] Correction for 2021–22: ACCC figures relating to authorisations for imposing a pecuniary penalty or protection of the public revenue have been amended due to a reporting error in the 2021–22 Annual Report. As such, the figures have been amended. Appendix D provides both the original figures reported for the 2021–22 period, and the amended figures as identified and amended by ACCC.

Agency	Authorisations	
	21/22	22/23
NSW Police	1,584[22]	1,299
NT Police	35	1
TAS Police	9	3
WA Police	18	7
TOTAL	**1,751[23]**	**1,347**

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 3 years. Prospective data authorisations may also authorise the disclosure of historical data.

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 reporting period.

This information is presented in **Table 33**. In 2022–23, there were 44,479 prospective data authorisations made by agencies under section 180 of the TIA Act. This is an increase of 6,382 on the 38,097 authorisations made in 2021–22.

[22] Correction for 2021–22: NSW Police figures relating to authorisations for imposing a pecuniary penalty or protection of the public revenue have been amended due to a reporting error in the 2021–22 Annual Report. As such, the figures have been amended. Appendix D provides both the original figures reported for the 2021–22 period, and the amended figures as identified and amended by NSW Police.
[23] Correction for 2021–22: ACCC and NSW Police figures relating to authorisations for imposing a pecuniary penalty or protection of the public revenue have been amended due to a reporting error in the 2021–22 Annual Report. As such, the figures have been amended. Appendix D provides both the original figures reported for the 2021–22 period, and the amended figures as identified and amended by these agencies.

Table 33: Total number of prospective data authorisations made – paragraph 186(1)(c)

Agency	Number of authorisations made	
	21/22	22/23
ACLEI	75	36
ACCC	3	4
ACIC	1,220	1,526
AFP	5,190	7,863
ASIC	89	36
CCC (WA)	49	29
Home Affairs	318	299
IBAC	158	170
ICAC (NSW)	4	36
ICAC (SA)	5	-
LECC	107	161
NSW CC	926	781
NSW Police	1,984	3,365
NT Police	449	403
QLD CCC	203	76
QLD Police	4,131	4,989
SA Police	324	452
TAS Police	117	118
VIC Police	18,936	18,733[24]
WA Police	3,809	5,402
TOTAL	**38,097**	**44,479**

[24] Note the Victoria Police has reported that 63 of these authorisations were inadvertently given for missing persons. Consequently, the total number of prospective data authorisations is reported as larger than the total number of offences associated with this at Table 36B on pages 77-78.

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 the Australian Security Intelligence Organisation (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.

In 2022–23, the AFP made the following authorisations under section 180A, 180B, 180C, and 180D of the TIA Act:

- 91 authorisations under section 180A
- no authorisations under section 180B
- 6 authorisations under section 180C, and
- no authorisations under section 180D.

Offences for which authorisations were made

Paragraph 186(1)(e) and subsection 186(2) of the TIA Act provide 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 34, 34A, 34B, 34C, 35, 36, 36A, 36B, and 36C**.

Under section 178A of the TIA Act, 6,119 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 34: Offences for which authorisations were made under section 178 to access existing data to enforce the criminal law – paragraph 186(1)(e)

Category of offences	Commonwealth agencies	State and Territory Police	State and Territory Integrity Agencies	TOTAL
Abduction	199	32,352	41	**32,592**
Acts – injury	116	15,005	-	**15,121**
Bribery or corruption	372	209	909	**1,490**
Cartel offences	42	15	-	**57**
Conspire	29	746	-	**775**
Cybercrime	964	3,183	9	**4,156**
Dangerous acts	20	5,412	-	**5,432**
Fraud	1,390	26,201	632	**28,223**
Homicide	783	31,673	349	**32,805**
Illicit drug offences	8,007	54,566	1,331	**63,904**
Loss of life	22	1,214	4	**1,240**
Misc.	797	12,796	123	**13,716**
Justice procedures	331	2,391	36	**2,758**
Organised offences	451	2,887	13	**3,351**
Pecuniary penalty	-	1,040	-	**1,040**
Public revenue	-	70	-	**70**
People smuggling	263	16	2	**281**

Category of offences	Commonwealth agencies	State and Territory Police	State and Territory Integrity Agencies	TOTAL
Weapons	435	4,897	56	**5,388**
Property damage	26	1,133	-	**1,159**
Public order offences	23	1,175	-	**1,198**
Robbery	131	17,099	24	**17,254**
Serious damage	5	4,976	-	**4,981**
Sexual assault	2,602	20,676	6	**23,284**
Special ACC investigation	4,293	81	-	**4,374**
Terrorism offences	671	672	138	**1,481**
Theft	378	23,818	-	**24,196**
Traffic	3	2,430	-	**2,433**
Unlawful entry	112	34,122	-	**34,234**
TOTAL	**22,465**	**300,855**	**3,673**	**326,993**

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

Categories of offences	ACLEI	ACCC	ACIC	AFP	ASIC	Home Affairs	TOTAL
Abduction	-	-	-	199	-	-	**199**
Acts – injury	-	-	-	116	-	-	**116**
Bribery or corruption	314	-	-	58	-	-	**372**
Cartel offences	-	42	-	-	-	-	**42**
Conspire	-	-	-	27	2	-	**29**
Cybercrime	-	-	-	925	39	-	**964**
Dangerous acts	-	-	-	20	-	-	**20**
Fraud	32	2	29	1,079	229	19	**1,390**
Homicide	-	-	-	783	-	-	**783**
Illicit drug offences	29	-	539	5,892	-	1,547	**8,007**
Loss of life	-	-	-	22	-	-	**22**
Misc.	4	-	-	230	18	545	**797**
Justice procedures	79	-	-	218	5	29	**331**
Organised offences	-	-	28	422	1	-	**451**
People smuggling	-	-	-	263	-	-	**263**
Weapons	-	-	8	124	-	303	**435**
Property damage	-	-	-	26	-	-	**26**

Categories of offences	ACLEI	ACCC	ACIC	AFP	ASIC	Home Affairs	TOTAL
Public order offences	-	-	-	23	-	-	**23**
Robbery	-	-	-	131	-	-	**131**
Serious damage	-	-	-	5	-	-	**5**
Sexual assault	-	-	-	2,602	-	-	**2,602**
Special ACC investigation	-	-	4,293	-	-	-	**4,293**
Terrorism offences	-	-	-	671	-	-	**671**
Theft	-	-	-	353	3	22	**378**
Traffic	-	-	-	3	-	-	**3**
Unlawful entry	-	-	-	112	-	-	**112**
TOTAL	**458**	**44**	**4,897**	**14,304**	**297**	**2,465**	**22,465**

Table 34B: State and Territory Police – Offences for which authorisations were made under section 178 to access existing data to enforce the criminal law – paragraph 186(1)(e)

Categories of offences	NSW Police	NT Police	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Abduction	10,947	268	3,927	317	319	14,097	2,477	**32,352**
Acts – injury	7,647	28	-	116	71	5,300	1,843	**15,005**
Bribery or corruption	-	-	-	37	-	105	67	**209**

Categories of offences	NSW Police	NT Police	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Cartel offences	15	-	-	-	-	-	-	**15**
Conspire	119	64	1	2	-	472	88	**746**
Cybercrime	2,030	28	756	7	53	35	274	**3,183**
Dangerous acts	845	44	1,464	255	18	2,284	502	**5,412**
Fraud	11,598	62	650	552	169	11,106	2,064	**26,201**
Homicide	18,911	213	1,768	1,354	612	7,298	1,517	**31,673**
Illicit drug offences	20,238	917	3,812	2,465	2,082	18,948	6,104	**54,566**
Loss of life	463	3	685	5	7	51	-	**1,214**
Misc.	5,081	106	6,849	21	23	362	354	**12,796**
Justice procedures	514	13	-	53	39	908	864	**2,391**
Organised offences	2,249	2	1	26	-	14	595	**2,887**
Pecuniary penalty	1,037	0	-	-	-	3	-	**1,040**
Public revenue	-	0	-	-	-	70	-	**70**
People smuggling	-	15	-	1	-	-	-	**16**
Weapons	1,771	-	40	166	41	2,837	42	**4,897**
Property damage	994	8	-	85	14	32	-	**1,133**
Public order offences	224	-	36	-	-	792	123	**1,175**
Robbery	7,054	41	1,459	233	81	5,799	2,432	**17,099**
Serious damage	1,318	17	733	7	29	2,309	563	**4,976**

Categories of offences	NSW Police	NT Police	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Sexual assault	8,423	306	1,960	726	117	6,776	2,368	**20,676**
Special ACC investigation	-	-	81	-	-	-	-	**81**
Terrorism offences	210	-	-	-	-	439	23	**672**
Theft	7,326	16	1,332	243	303	11,498	3,100	**23,818**
Traffic	573	-	296	15	13	1,241	292	**2,430**
Unlawful entry	3,491	7	1,813	340	122	19,973	8,376	**34,122**
TOTAL	**113,078**	**2,158**	**27,663**	**7,026**	**4,113**	**112,749**	**34,068**	**300,855**

Table 34C: State and Territory Integrity Agencies – Offences for which authorisations were made under section 178 to access existing data to enforce the criminal law – paragraph 186(1)(e)

Categories of offences	CS NSW	CCC (WA)	IBAC	ICAC (NSW)	ICAC (SA)	LECC	NSW CC	QLD CCC	TOTAL
Abduction	-	-	-	-	-	8	33	-	**41**
Bribery or corruption	-	99	263	16	111	344	-	76	**909**
Cybercrime	-	-	-	-	-	7	-	2	**9**
Fraud	-	-	14	103	-	107	371	37	**632**
Homicide	-	-	-	-	-	-	349	-	**349**
Illicit drug offences	1	-	-	-	-	30	1,141	159	**1,331**

Categories of offences	CS NSW	CCC (WA)	IBAC	ICAC (NSW)	ICAC (SA)	LECC	NSW CC	QLD CCC	TOTAL
Loss of life	-	-	-	-	-	-	4	-	**4**
Misc.	2	7	-	-	-	-	40	74	**123**
Justice procedures	-	3	9	5	-	19	-	-	**36**
Organised offences	-	-	-	-	-	-	13	-	**13**
People smuggling	-	-	-	-	-	-	2	-	**2**
Weapons	-	-	-	-	-	-	56	-	**56**
Robbery	-	-	-	1	-	-	23	-	**24**
Sexual assault	-	-	-	-	-	-	1	5	**6**
Terrorism offences	-	-	-	-	-	-	138	-	**138**
TOTAL	**3**	**109**	**286**	**125**	**111**	**515**	**2,171**	**353**	**3,673**

Table 35: 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	AFP	ASIC	Home Affairs	NSW Police	NT Police	TAS Police	WA Police	TOTAL
Abduction	-	-	-	68	-	-	-	**68**
Acts – injury	-	-	-	14	-	-	-	**14**
Cartel offences	-	-	-	7	-	-	-	**7**
Cybercrime	-	-	-	7	-	-	-	**7**

Categories of offences	AFP	ASIC	Home Affairs	NSW Police	NT Police	TAS Police	WA Police	TOTAL
Dangerous acts	-	-	-	26	-	-	-	**26**
Fraud	-	5	-	31	-	-	-	**36**
Homicide	-	-	-	160	-	-	-	**160**
Illicit drug offences	-	-	1	59	-	-	-	**60**
Loss of life	-	-	-	11	-	-	-	**11**
Miscellaneous	-	-	1	20	-	-	-	**21**
Justice procedures	-	-	-	4	1	-	6	**11**
Organised offences	-	-	-	10	-	-	-	**10**
Pecuniary penalty	10	2	17	246	-	-	-	**275**
People smuggling	-	-	-	1	-	-	-	**1**
Weapons	-	-	1	12	-	1	-	**14**
Property damage	-	-	-	11	-	-	-	**11**
Robbery	-	-	-	540	-	-	-	**540**
Sexual assault	-	-	-	35	-	-	-	**35**
Terrorism offences	-	-	-	1	-	-	-	**1**
Theft	-	-	-	24	-	-	-	**24**
Traffic offences	-	-	-	12	-	2	1	**15**
TOTAL	**10**	**7**	**20**	**1,299**	**1**	**3**	**7**	**1,347**

Table 36: 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	Commonwealth agencies	State and Territory Police	State and Territory Integrity Agencies	TOTAL
Abduction	54	3,200	1	**3,255**
Acts – injury	34	2,165	-	**2,199**
Bribery or corruption	59	34	318	**411**
Cartel offences	3	-	-	**3**
Conspire	17	147	1	**165**
Cybercrime	176	39	3	**218**
Dangerous acts	9	480	-	**489**
Fraud	830	1,296	193	**2,319**
Homicide	334	1,125	76	**1,535**
Illicit drug offences	3,510	9,625	416	**13,551**
Loss of life	8	61	-	**69**
Misc.	232	607	122	**961**
Justice procedures	77	304	2	**383**
Organised offences	3,151	48	9	**3,208**
Public revenue	56	8	-	**64**
People smuggling	99	4	-	**103**
Weapons	161	1,216	72	**1,449**

Categories of offences	Commonwealth agencies	State and Territory Police	State and Territory Integrity Agencies	TOTAL
Property damage	5	132	-	**137**
Public order offences	-	126	-	**126**
Robbery	59	1,795	3	**1,857**
Serious damage	7	471	-	**478**
Sexual assault	289	1,443	1	**1,733**
Special ACC investigation	416	-	-	**416**
Terrorism offences	163	147	36	**346**
Theft	205	3,534	-	**3,739**
Traffic	20	148	-	**168**
Unlawful entry	29	5,244	-	**5,273**
TOTAL	**10,003**	**33,399**	**1,253**	**44,655**

Table 36A: Commonwealth agencies – 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	ACLEI	ACCC	ACIC	AFP	ASIC	Home Affairs	TOTAL
Abduction	-	-	-	54	-	-	**54**
Acts – injury	-	-	-	34	-	-	**34**
Bribery or corruption	38	-	-	21	-	-	**59**

Categories of offences	ACLEI	ACCC	ACIC	AFP	ASIC	Home Affairs	TOTAL
Cartel offences	-	3	-	-	-	-	**3**
Conspire	-	-	1	16	-	-	**17**
Cybercrime	-	-	11	164	1	-	**176**
Dangerous acts	-	-	-	9	-	-	**9**
Fraud	-	1	424	372	33	-	**830**
Homicide	-	-	-	334	-	-	**334**
Illicit drug offences	7	-	537	2,842	-	124	**3,510**
Loss of life	-	-	-	8	-	-	**8**
Misc.	10	-	-	134	6	82	**232**
Justice procedures	20	-	-	51	6	-	**77**
Organised offences	-	-	87	3,064	-	-	**3,151**
Public revenue	-	-	54	2	-	-	**56**
People smuggling	-	-	-	99	-	-	**99**
Weapons	-	-	3	70	-	88	**161**
Property damage	-	-	-	5	-	-	**5**
Robbery	-	-	-	59	-	-	**59**
Serious damage	-	-	-	7	-	-	**7**
Sexual assault	-	-	-	289	-	-	**289**
Special ACC investigation	-	-	416	-	-	-	**416**

Categories of offences	ACLEI	ACCC	ACIC	AFP	ASIC	Home Affairs	TOTAL
Terrorism offences	-	-	-	163	-	-	**163**
Theft	-	-	-	199	1	5	**205**
Traffic	-	-	-	20	-	-	**20**
Unlawful entry	-	-	-	29	-	-	**29**
TOTAL	**75**	**4**	**1,533**	**8,045**	**47**	**299**	**10,003**

Table 36B: State and Territory Police – 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	NSW Police	NT Police	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Abduction	218	32	654	38	4	2,110	144	**3,200**
Acts – injury	384	17	-	16	-	1,503	245	**2,165**
Bribery or corruption	4	-	3	-	-	27	-	**34**
Conspire	13	11	-	-	-	87	36	**147**
Cybercrime	11	6	11	-	-	1	10	**39**
Dangerous acts	19	7	39	9	-	406	-	**480**
Fraud	99	1	137	1	-	831	227	**1,296**
Homicide	168	39	218	42	28	556	74	**1,125**
Illicit drug offences	1,108	233	2,546	220	72	3,488	1,958	**9,625**

Categories of offences	NSW Police	NT Police	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Loss of life	35	1	9	1	-	15	-	**61**
Misc.	253	3	74	1	2	18	256	**607**
Justice procedures	35	-	2	-	-	119	148	**304**
Organised offences	32	-	8	8	-	-	-	**48**
Public revenue	-	-	-	-	-	8	-	**8**
People smuggling	-	4	-	-	-	-	-	**4**
Weapons	159	-	117	22	-	855	63	**1,216**
Property damage	34	-	8	-	-	14	76	**132**
Public order offences	8	-	-	-	-	117	1	**126**
Robbery	233	7	312	13	2	857	371	**1,795**
Serious damage	22	4	95	-	-	331	19	**471**
Sexual assault	104	32	152	52	5	904	194	**1,443**
Terrorism offences	21	-	1	-	-	125	-	**147**
Theft	209	2	249	13	4	2,560	497	**3,534**
Traffic	13	-	-	-	1	121	13	**148**
Unlawful entry	183	4	354	16	-	3,617	1,070	**5,244**
TOTAL	**3,365**	**403**	**4,989**	**452**	**118**	**18,670**	**5,402**	**33,399**

Table 36C: State and Territory Integrity Agencies – 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	CCC (WA)	IBAC	ICAC (NSW)	LECC	NSW CC	QLD CCC	TOTAL
Abduction	-	-	-	-	1	-	**1**
Bribery or corruption	20	163	1	129	-	5	**318**
Conspire	-	-	-	-	1	-	**1**
Cybercrime	-	-	-	3	-	-	**3**
Fraud	-	6	34	25	124	4	**193**
Homicide	-	-	-	-	76	-	**76**
Illicit drug offences	-	-	-	2	369	45	**416**
Misc.	9	1	-	-	91	21	**122**
Justice procedures	-	-	-	2	-	-	**2**
Organised offences	-	-	-	-	9	-	**9**
Weapons	-	-	-	-	72	-	**72**
Robbery	-	-	1	-	2	-	**3**
Sexual assault	-	-	-	-	-	1	**1**
Terrorism offences	-	-	-	-	36	-	**36**
TOTAL	**29**	**170**	**36**	**161**	**781**	**76**	**1,253**

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 37**. The statistics are split into successive periods of 3 months and include the total number of authorisations made for data held for lengths of time specified, in accordance with subsection 180(1C) of the TIA Act.

In 2022–23, there were 283,248 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, which have been recorded as '0' months old and are included in the 0–3 month field.[25]

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

Table 37: Periods for which retained data was held by carrier before authorised disclosure – paragraph 186(1)(f)

Agency	Age of disclosure									
	0-3 months	3-6 months	6-9 months	9-12 months	12-15 months	15-18 months	18-21 months	21-24 months	Over 24 months	TOTAL
ACLEI	202	32	4	27	8	1	6	10	55	**345**
ACCC	3	-	3	10	2	2	3	0	21	**44**
ACIC	3,815	492	211	97	166	36	17	10	69	**4,913**
AFP	6,262	3,208	1,532	871	853	274	295	174	1,015	**14,484**
ASIC	190	14	7	3	5	3	7	8	45	**282**
CS NSW	-	-	-	1	1	-	-	-	-	**2**
CCC (WA)	74	5	7	3	2	-	1	3	14	**109**
Home Affairs	1,819	325	140	73	67	10	6	4	41	**2,485**
IBAC	426	11	1	6	-	1	-	2	3	**450**
ICAC (NSW)	42	6	6	5	2	1	3	4	56	**125**
ICAC (SA)	7	22	14	19	18	2	2	-	27	**111**
LECC	424	24	9	13	2	-	3	6	34	**515**
NSW CC	1,545	82	54	91	106	24	23	46	200	**2,171**

Agency	Age of disclosure									
	0-3 months	3-6 months	6-9 months	9-12 months	12-15 months	15-18 months	18-21 months	21-24 months	Over 24 months	TOTAL
NSW Police	106,817	2,843	1,703	1,505	734	604	626	527	1,727	**117,086**
NT Police	1,980	92	33	16	23	10	10	6	25	**2,195**
QLD CCC	170	76	25	42	13	1	5	-	21	**353**
QLD Police	23,462	1,655	848	515	403	229	169	123	620	**28,024**
SA Police	4,856	724	314	243	181	49	89	124	574	**7,154**
TAS Police	4,616	430	103	44	67	37	20	10	91	**5,418**
VIC Police	99,660	6,107	2,610	1,330	1,070	501	439	282	1,884	**113,883**
WA Police	26,878	2,690	1,405	745	639	354	219	247	1,271	**34,448**
TOTAL	**283,248**	**18,838**	**9,029**	**5,659**	**4,362**	**2,139**	**1,943**	**1,586**	**7,793**	**334,597**

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 38: Types of retained data disclosed in authorisations – paragraphs 186(1)(g) and 186(1)(h)[26]

Agency	Item 1: subscriber data	Items 2-6: traffic data
ACLEI	82	334
ACCC	28	16
ACIC	3,106	1,812
AFP	11,657	2,730
ASIC	158	88
CS NSW	2	2
CCC (WA)	64	45
Home Affairs	1,895	1,137
IBAC	219	108
ICAC (NSW)	78	47
ICAC (SA)	35	76
LECC	426	89
NSW CC	1,129	1,167
NSW Police	79,770	53,284

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

Agency	Item 1: subscriber data	Items 2-6: traffic data
NT Police	1,535	485
QLD CCC	237	116
QLD Police	19,448	6,845
SA Police	5,607	1,547
TAS Police	4,322	1,096
VIC Police	43,564	70,319
WA Police	25,301	9,147
TOTAL	**198,663**	**150,490**

Journalist information warrants

The journalist information warrant (JIW) scheme requires agencies to obtain a JIW prior to authorising the disclosure of telecommunications data relating to a 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 reporting period and the number of authorisations made under JIWs issued to those agencies.

In 2022–23, no JIWs were issued and no authorisations were made under a JIW. This is consistent with 2021–22.

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 Parliamentary Joint Committee on Intelligence and Security (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. The Government is committed to implementing these recommendations. Ahead of legislative amendments, the Government has included information about the number of PIAs, their location and qualification in **Table 39**.

Table 39: Public interest advocates

Public interest advocate	Location	Qualification
1	Queensland	Former Judge
2	Victoria	Former Judge
3	Northern Territory	Senior Counsel
4	Western Australia	Former Judge
5	South Australia	King's Counsel
6	South Australia	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 and 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, shows the cost of complying with the data retention obligations.

This information is set out in **Table 40**. **Table 40** further sets out the costs recovered from criminal law-enforcement agencies for the purpose of complying with their data retention obligations.

Table 40: 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)
2021–22	$28,136,658.54	$13,385,407.50
2022–23	$26,019,314.37	$15,171,490.00

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 communications 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, a transmission service provider, a message/call application service provider, 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 2022–23, no IPOs were issued in this reporting period.

As at 30 June 2023, the *Agreement between the Government of Australia and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime* (currently the only agreement under the International Production Order framework), had not entered into force.

Paragraph 131(1)(b) of Schedule 1 provides that this report must set out information relating to the Australian Designated Authority. **Table 41** reflects that no IPOs were issued in 2022–23.

Table 41: Annual report by the Australian Designated Authority – clause 131

Australian Designated Authority 2022–23 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 the Australian Designated Authority to prescribed communications providers (clause 130(1)(a)(iii))	0
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

Australian Designated Authority 2022–23 Annual Report	
Reporting item	**Number for each agency**
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 framework 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 provides a graduated approach for agencies to receive assistance from industry through the use of three powers:

- **Technical Assistance Request (TAR):** Agencies can request voluntary help from designated communications providers.[27]
- **Technical Assistance Notice (TAN):** Agencies can require designated communication providers to give help where they already have the technical capability to do so.
- **Technical Capability Notice (TCN):** Agencies can require designated communications providers to give help, including in circumstances where they may not have the technical capability to do so.

Table 42: Eligible agencies under Part 15 of the Telecommunications Act

Agency	Industry assistance powers available to agencies		
	TAR	TAN	TCN
Interception agencies[28]	✓	✓	✓
ASD	✓	×	×
ASIO	✓	✓	✓
ASIS	✓	×	×

[27] Categories of designated communications providers and their eligible activities are at section 317C of the Telecommunications Act.
[28] In contrast to the TIA Act, this does not include anti-corruption and integrity commissions.

Definition

'Interception agency' for the purposes of Part 15 of the Telecommunications Act means the AFP, the ACIC, and the police force of a state or the Northern Territory.

The industry assistance framework provides that:

- any assistance or capability requested must be reasonable, proportionate, practicable and technically feasible, and
- assistance to law enforcement must be related to investigating serious Australian offences or assisting the enforcement of serious foreign offences, or safeguarding national security.

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 3 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 3 years or more, or for life.

The framework contains numerous limitations and safeguards including:

- prohibiting assistance that creates 'systemic weaknesses' in encrypted devices and communications systems
    - this includes a prohibition on requesting or requiring providers to refrain from fixing vulnerabilities or making their systems more secure, building a decryption capability, or reducing the broader security of their systems
- prohibiting the doing of things that could otherwise require agencies to obtain a warrant or authorisation under the relevant law of the Commonwealth, State or Territory 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 reporting period, and the number of TCNs given during the reporting period that were directed towards ensuring designated communications providers were capable of giving help to interception agencies.

This information is presented in **Table 43**. In 2022–23, 66 TARs were given by interception agencies to designated communications providers. This increased by 36 from the previous year.

Table 43: 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					
	TAR		TAN		TCN	
	21/22	22/23	21/22	22/23	21/22	22/23
ACIC	4	6	-	-	-	-
AFP	2	-	-	-	-	-
NSW Police	21	53	-	-	-	-
QLD Police	-	1	-	-	-	-
VIC Police	3	5	-	-	-	-
WA Police	-	1	-	-	-	-
TOTAL	**30**	**66**	**-**	**-**	**-**	**-**

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 reporting period 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 44**.

Table 44: Kinds of serious Australian offences enforced through Technical Assistance Requests – paragraph 317ZS(1)(d) of the Telecommunications Act

Categories of offences	ACIC	NSW Police	QLD Police	VIC Police	WA Police	TOTAL
Special ACIC Investigation	6	-	-	-	-	**6**
Acts intended to cause injury	-	-	-	1	-	**1**
Fraud, deception and related offences	-	2	-	-	-	**2**
Homicide and related offences	-	36	-	-	-	**36**
Illicit drug offences	-	11	-	-	-	**11**
Property damage and environment pollution	-	1	-	-	-	**1**
Robbery, extortion and related offences	-	3	-	-	-	**3**
Sexual assault and related offences	-	-	-	4	1	**5**
Other serious Australian offences	-	-	1	-	-	**1**
TOTAL	**6**	**53**	**1**	**5**	**1**	**66**

Oversight of industry assistance powers

Use of the industry assistance powers 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 its 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 (as well as other Acts), the Ombudsman considers agency use of these powers collectively.

Where a state or territory law enforcement agencies 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 the ASIO, the Australian Signals Directorate and the Australian Secret Intelligence Service, this is the IGIS. In the case of interception agencies, this is the Ombudsman. Additionally, in the case of police forces of a state and the Northern Territory, 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.

Chapter 7: Further information

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

Electronic Surveillance Section

Attorney-General's Department

3-5 NATIONAL CIRCUIT

BARTON ACT 2600

ElectronicSurveillance@ag.gov.au

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

Previous copies of the Annual Report under the *Telecommunications (Interception and Access) Act 1979* and Part 15 of *Telecommunications Act 1997* 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 (ACLEI)
Australian Criminal Intelligence Commission (ACIC)
Australian Federal Police (AFP)
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)
Independent Commissioner Against Corruption (South Australia)
Law Enforcement Conduct Commission (New South Wales)
New South Wales Crime Commission
New South Wales Police Force
Northern Territory Police Force
Queensland Police Service
South Australia 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, paragraphs 5D(1)(e), (ic), (id), (if), (ig), (vii) and (viii)
Kidnapping	TIA Act, paragraph 5D(1)(b)
Loss of life or personal injury	TIA Act, subparagraphs 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, subsections 5D(3AA), (8A) and (9)
People smuggling and related offences	TIA Act, subsection 5D(3A)
Serious damage to property and/or serious arson	TIA Act, subparagraphs 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 or 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: Updated figures for previous reporting periods

ACCC 2021–22

ACCC identified corrections regarding access to telecommunications data for the 2021–22 reporting period. These errors were detected following an inspection by the Commonwealth Ombudsman and included one database error and two authorisations dated 4 July 2022 which were incorrectly counted for the 2021–22 reporting period.

The below tables detail both the original figures provided for the previous 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)[29]

Agency	Authorisations	
	21/22 Original	21/22 Updated
ACCC	34	31
TOTAL	**304,652**	**306,559**[30]

[29] Correction refers to Table 31, page 50, 2021–22 Annual Report under the TIA Act and Part 15 of the Telecommunications Act.
[30] This figure includes updates identified by other agencies in Appendix D of this Annual Report.

Number of 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)[31]

Agency	Authorisations	
	21/22 Original	21/22 Updated
ACCC	5	6
TOTAL	**1,734**	**1,751**[32]

Offences for which authorisations were made under section 178 to access existing data to enforce the criminal law – paragraph 186(1)(e)[33]

Categories of offences	21/22 Original	21/22 Updated
Cartel offences	34	31
TOTAL (ACCC)	**34**	**31**

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)[34]

Categories of offences	21/22 Original	21/22 Updated
Cartel offences	2	3
TOTAL (ACCC)	**5**	**6**

[31] Correction refers to Table 33, page 52, 2021–22 Annual Report under the TIA Act and Part 15 of the Telecommunications Act.
[32] This figure includes updates identified by other agencies in Appendix D of this Annual Report.
[33] Correction refers to Table 35, page 55, 2021–22 Annual Report under the TIA Act and Part 15 of the Telecommunications Act.
[34] Correction refers to Table 36, pages 57-58, 2021–22 Annual Report under the TIA Act and Part 15 of the Telecommunications Act.

Periods for which retained data was held by carrier before authorised disclosure – paragraph 186(1)(f)[35]

ACCC	Age of disclosure									
	0-3 months	3-6 months	6-9 months	9-12 months	12-15 months	15-18 months	18-21 months	21-24 months	Over 24 months	TOTAL
21/22 Original	2	-	5	9	1	2	-	9	11	**39**
21/22 Updated	2	-	5	9	1	-	-	9	11	**37**

Types of retained data disclosed in authorisations – paragraphs 186(1)(g) and 186(1)(h)[36]

ACCC	Item 1: subscriber data	Items 2-6: traffic data
21/22 Original	19	20
21/22 Updated	19	18

[35] Correction refers to Table 38, page 61, 2021–22 Annual Report under the TIA Act and Part 15 of the Telecommunications Act.
[36] Correction refers to Table 39, page 63, 2021–22 Annual Report under the TIA Act and Part 15 of the Telecommunications Act.

AFP 2017–18 and 2021–22

In the 2021–22 Annual Report, AFP corrected a number of errors regarding access to telecommunications data for the 2016–17 to 2020–21 reporting periods. Following provision of the 2021–22 Annual Report to the Attorney-General, the AFP identified further errors in relation to offences for which authorisations were made to access existing data to enforce the criminal law. AFP advised these errors occurred due to an administrative transposing error.

Offences for which authorisations were made to access existing data to enforce the criminal law – paragraph 186(1)(e)[37]

Categories of offences	17/18 Original	17/18 Updated
Abduction	456	656
Bribery or corruption	110	107
Cybercrime	179	1,878
Dangerous acts	133	135
Fraud	947	950
Illicit drug offences	8,200	10,198
Loss of life	6	8
Justice procedures	327	308
Organised offences	476	495
Pecuniary penalty	43	39
Public revenue	7	11
Sexual assault	415	412
Terrorism offences	1,627	1,630
Theft	294	293
Traffic	57	59
Unlawful entry	-	107

[37] Correction refers to Table 33, pages 53-4, 2017–18 TIA Act Annual Report.

Categories of offences	17/18 Original	17/18 Updated
TOTAL (AFP)[38]	**15,425**	**19,434**

AGD identified that the figures regarding the number of data authorisations made for foreign law enforcement purposes were omitted from the 2021–22 Annual Report due to an internal administrative error. The below details the figures that were incorrectly omitted from the 2021–22 Annual Report.[39]

In 2021–22, the AFP made the following authorisations under section 180A, 180B, 180C, and 180D of the TIA Act:

- 34 authorisations under section 180A
- 1 authorisation under section 180B
- 2 authorisations under section 180C, and
- no authorisations under section 180D.

[38] Categories without corrections have not been replicated in the table.
[39] Correction refers to page 54, 2021–22 Annual Report under the TIA Act and Part 15 of the Telecommunications Act.

IBAC 2021–22

IBAC identified corrections regarding access to telecommunications data for the 2021–22 reporting period. These errors were detected following an inspection by the Ombudsman in March 2023 where it was identified that 7 telecommunications data authorisations were not included in the information provided by IBAC due to a system limitation which did not allow the counting of telecommunications data requests that had been authorised but were never sent to the carrier.

The below tables detail both the original figures provided for the previous 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)[40]

Agency	Authorisations	
	21/22 Original	21/22 Updated
IBAC	337	344
TOTAL	**304,652**	**306,559**[41]

Offences for which authorisations were made under section 178 to access existing data to enforce the criminal law – paragraph 186(1)(e)[42]

Categories of offences	21/22 Original	21/22 Updated
Bribery or corruption	315	322
TOTAL (IBAC)	**337**	**344**

[40] Correction refers to Table 31, page 50, 2021–22 Annual Report under the TIA Act and Part 15 of the Telecommunications Act.
[41] This figure includes updates identified by other agencies in Appendix D of this Annual Report.
[42] Correction refers to Table 35, page 55, 2021–22 Annual Report under the TIA Act and Part 15 of the Telecommunications Act.

Periods for which retained data was held by carrier before authorised disclosure – paragraph 186(1)(f)[43]

IBAC	Age of disclosure									
	0-3 months	3-6 months	6-9 months	9-12 months	12-15 months	15-18 months	18-21 months	21-24 months	Over 24 months	TOTAL
21/22 Original	263	10	13	4	4	1	4	5	33	**337**
21/22 Updated	269	10	13	5	4	1	4	5	33	**344**

Types of retained data disclosed in authorisations – paragraphs 186(1)(g) and 186(1)(h)[44]

IBAC	Item 1: subscriber data	Items 2-6: traffic data
21/22 Original	230	123
21/22 Updated	233	128

[43] Correction refers to Table 38, page 61, 2021–22 Annual Report under the TIA Act and Part 15 of the Telecommunications Act.
[44] Correction refers to Table 39, page 63, 2021–22 Annual Report under the TIA Act and Part 15 of the Telecommunications Act.

NSW Police 2021–22

NSW Police identified corrections regarding access to telecommunications data for the 2021–22 reporting period. These errors were detected following an inspection by the Ombudsman of the 2021–22 records where it was identified that a large number of records were unable to be matched due to a system error caused by a previous system upgrade. The system error has since been rectified.

The below tables detail both the original figures provided for the previous 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)[45]

Agency	Authorisations	
	21/22 Original	21/22 Updated
NSW Police	103,239	105,142
TOTAL	**304,652**	**306,559**[46]

[45] Correction refers to Table 31, page 50, 2021–22 Annual Report under the TIA Act and Part 15 of the Telecommunications Act.
[46] This figure includes updates identified by other agencies in Appendix D of this Annual Report.

Authorisations made for access to existing information or documents for the location of missing persons – paragraph 186(1)(aa)[47]

Agency	Authorisations	
	21/22 Original	21/22 Updated
NSW Police	2,515	2,529
TOTAL	**4,207**	**4,222**[48]

Number of 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)[49]

Agency	Authorisations	
	21/22 Original	21/22 Updated
NSW Police	1,568	1,584
TOTAL	**1,734**	**1,751**[50]

Offences for which authorisations were made under section 178 to access existing data to enforce the criminal law – paragraph 186(1)(e)[51]

Categories of offences	21/22 Original	21/22 Updated
Abduction	7,426	7,516
Acts – injury	4,859	5,019

[47] Correction refers to Table 32, page 51, 2021–22 Annual Report under the TIA Act and Part 15 of the Telecommunications Act.
[48] This figure includes updates identified by other agencies in Appendix D of this Annual Report.
[49] Correction refers to Table 33, page 52, 2021–22 Annual Report under the TIA Act and Part 15 of the Telecommunications Act.
[50] This figure includes updates identified by other agencies in Appendix D of this Annual Report.
[51] Correction refers to Table 35, page 55, 2021–22 Annual Report under the TIA Act and Part 15 of the Telecommunications Act.

Categories of offences	21/22 Original	21/22 Updated
Conspire	202	203
Cybercrime	2,226	2,246
Dangerous acts	820	839
Fraud	13,121	13,233
Homicide	16,671	16,944
Illicit drug offences	22,231	22,851
Loss of life	488	494
Miscellaneous	4,915	4,947
Justice procedures	692	696
Organised offences	2,101	2,132
Pecuniary penalty	768	772
Weapons	1,273	1,332
Property damage	1,630	1,659
Public order offences	527	538
Robbery	6,786	6,917
Serious damage	417	426
Sexual assault	8,021	8,185
Terrorism	182	189
Theft	4,955	5,042
Traffic	638	643
Unlawful entry	2,280	2,309
TOTAL (NSW Police)[52]	**103,239**	**105,142**

[52] Categories without corrections have not been replicated in the table.

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)[53]

Categories of offences	21/22 Original	21/22 Updated
Homicide	182	186
Illicit drug offences	97	100
Loss of life	7	8
Miscellaneous	47	48
Pecuniary penalty	419	423
Robbery	508	509
Theft	95	97
TOTAL (NSW Police)[54]	**1,568**	**1,584**

[53] Correction refers to Table 36, pages 57-58, 2021–22 Annual Report under the TIA Act and Part 15 of the Telecommunications Act.
[54] Categories without corrections have not been replicated in the table.

Periods for which retained data was held by carrier before authorised disclosure – paragraph 186(1)(f)[55]

NSW Police	Age of disclosure									
	0-3 months	3-6 months	6-9 months	9-12 months	12-15 months	15-18 months	18-21 months	21-24 months	Over 24 months	TOTAL
21/22 Original	92,349	4,959	2,782	1,680	1,629	867	485	310	2,261	**107,322**
21/22 Updated	94,170	4,986	2,804	1,705	1,632	875	494	315	2,274	**109,255**

Types of retained data disclosed in authorisations – paragraphs 186(1)(g) and 186(1)(h)[56]

NSW Police	Item 1: subscriber data	Items 2-6: traffic data
21/22 Original	73,647	33,672
21/22 Updated	75,594	33,658

[55] Correction refers to Table 38, page 61, 2021–22 Annual Report under the TIA Act and Part 15 of the Telecommunications Act.
[56] Correction refers to Table 39, page 63, 2021–22 Annual Report under the TIA Act and Part 15 of the Telecommunications Act.

NT Police 2021–22

During the quality assurance process for the annual reporting statistics for the 2021–22 reporting period, NT Police provided a number of corrections to statistics provided for that reporting period, most of which were implemented before the 2021–22 Annual Report was provided to the Attorney-General. NT Police and AGD identified that the correction provided by NT Police regarding authorisations made for access to existing information or documents for the location of missing persons was not implemented due to an internal administrative error.

The below table details both the original figure provided for the previous annual report and the amended figure as identified and corrected.

Authorisations made for access to existing information or documents for the location of missing persons – paragraph 186(1)(aa)[57]

Agency	Authorisations	
	21/22 Original	21/22 Updated
NT Police	35	36
TOTAL	**4,207**	**4,222**[58]

[57] Correction refers to Table 32, page 51, 2021–22 Annual Report under the TIA Act and Part 15 of the Telecommunications Act.
[58] This figure includes updates identified by other agencies in Appendix D of this Annual Report.

VIC Police 2018–19 and 2019–20

VIC Police identified corrections regarding access to telecommunications data for the 2018–19 and 2019–20 reporting periods. These errors were identified following inspections by the Commonwealth Ombudsman in 2019 and 2020 which recommended reviews of VIC Police's telecommunications data holdings. During the first stage of these reviews, technical anomalies were identified within VIC Police's systems that resulted in the underreporting of authorisations. Work has commenced to eliminate these anomalies for future reporting periods.

The below tables detail both the original figures provided for the previous 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)

Agency	Authorisations			
	18/19 Original	18/19 Updated[59]	19/20 Original	19/20 Updated[60]
VIC Police	87,680	91,169	88,526	98,465
TOTAL	**289,644**[61]	**293,133**	**306,956**[62]	**316,895**

[59] Correction refers to Table 30, page 54, 2018–19 TIA Act Annual Report.
[60] Correction refers to Table 29, page 56, 2019–20 TIA Act Annual Report.
[61] This figure includes updates identified in Appendix D, page 79, 2021–22 Annual Report under the TIA Act and Part 15 of the Telecommunications Act.
[62] This figure includes updates identified in Appendix D, page 79, 2021–22 Annual Report under the TIA Act and Part 15 of the Telecommunications Act.

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

Agency	Authorisations			
	18/19 Original	18/19 Updated[63]	19/20 Original	19/20 Updated[64]
VIC Police	447	712	561	681
TOTAL	**2,574**	**2,839**	**3,028**	**3,148**

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

Agency	Number of authorisations made			
	18/19 Original	18/19 Updated[65]	19/20 Original	19/20 Updated[66]
VIC Police	11,219	12,066	14,801	14,788
TOTAL	**27,950[67]**	**28,797**	**32,934[68]**	**32,921**

[63] Correction refers to Table 31, page 55, 2018–19 TIA Act Annual Report.
[64] Correction refers to Table 30, page 57, 2019–20 TIA Act Annual Report.
[65] Correction refers to Table 33, page 55, 2018–19 TIA Act Annual Report.
[66] Correction refers to Table 32, page 60, 2019–22 TIA Act Annual Report.
[67] This figure includes updates identified in Appendix D, page 80, 2020–21 TIA Act Annual Report.
[68] This figure includes updates identified in Appendix D, page 80, 2020–21 TIA Act Annual Report.

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

Categories of offences	18/19 Original	18/19 Updated[69]	19/20 Original	19/20 Updated[70]
Abduction	1,044	5,822	2,908	4,523
Acts – injury	4,816	5,428	2,852	3,832
Bribery or corruption	79	565	67	541
Conspire	636	181	258	315
Cybercrime	957	910	1,386	1,661
Dangerous acts	2,186	1,784	2,682	2,703
Fraud	8,092	9,943	9,728	10,197
Homicide	5,833	4,302	6,282	6,613
Illicit drug offences	19,150	16,639	17,990	17,736
Loss of life	9	847	412	337
Miscellaneous	1,423	1,124	118	287
Justice procedures	999	6,244	2,466	7,853
Organised offences	-	1	88	10
Public revenue	-	27	-	145
People smuggling	-	3	-	3
Weapons	3,383	1,170	1,661	1,877
Property damage	2,496	2,271	1,996	1,974
Public order offences	-	23	260	18
Robbery	8,771	7,726	8,503	8,431
Serious damage	4	7	2	2
Sexual assault	4,798	4,332	5,180	4,250
Terrorism	977	686	451	483
Theft	7,940	8,606	8,796	9,787

[69] Corrections refer to Table 35, page 61, 2018–19 TIA Act Annual Report.
[70] Corrections refer to Table 34, page 63, 2019–20 TIA Act Annual Report.

Categories of offences	18/19 Original	18/19 Updated[69]	19/20 Original	19/20 Updated[70]
Traffic	967	285	1,048	965
Unlawful entry	13,129	12,243	13,392	13,922
TOTAL (VIC Police)[71]	**87,680**	**91,169**	**88,526**	**98,465**

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

Categories of offences	18/19 Original	18/19 Updated[72]	19/20 Original	19/20 Updated[73]
Abduction	-	4	-	-
Acts – injury	-	2	-	-
Dangerous acts	-	1	-	-
Fraud	-	7	-	-
Miscellaneous	-	1	-	-
Justice procedures	-	1	-	-
Property damage	-	1	-	-
Robbery	-	3	-	-
Theft	-	2	-	-
Traffic	-	1	-	-
Unlawful entry	-	5	-	-
No offence attached to s 178A authorisation	447	684	561	681
TOTAL (VIC Police)[74]	**447**	**712**	**561**	**681**

[71] Categories without corrections have not been replicated in the table.
[72] Corrections refer to Table 36, page 63, 2018–19 TIA Act Annual Report.
[73] Corrections refer to Table 35, page 65, 2019–20 TIA Act Annual Report.
[74] Categories without corrections have not been replicated in the table.

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

Categories of offences	18/19 Original	18/19 Updated[75]	19/20 Original	19/20 Updated[76]
Abduction	338	677	606	581
Acts – injury	871	1,012	841	825
Bribery or corruption	32	22	32	45
Conspire	27	30	43	15
Cybercrime	19	38	49	85
Dangerous acts	328	222	363	510
Fraud	615	404	563	562
Homicide	495	428	706	714
Illicit drug offences	3,470	3,368	3,381	3,354
Loss of life	47	76	8	67
Miscellaneous	-	68	26	63
Justice procedures	16	477	917	917
Organised offences	2	1	2	-
Public revenue	-	-	2	11
People smuggling	-	2	-	-
Weapons	509	337	546	579
Property damage	-	115	187	191
Public order offences	1	1	89	4
Robbery	976	831	1,234	1,216
Serious damage	209	8	17	17
Sexual assault	571	393	419	319
Terrorism offences	43	55	41	38

[75] Corrections refer to Table 38, page 67, 2018–19 TIA Act Annual Report.
[76] Corrections refer to Table 37, page 69, 2019–20 TIA Act Annual Report.

Categories of offences	18/19 Original	18/19 Updated[75]	19/20 Original	19/20 Updated[76]
Theft	1,160	1,709	1,937	1,941
Traffic	33	13	112	60
Unlawful entry	1,457	1,779	2,680	2,674
TOTAL (VIC Police)[77]	**11,219**	**12,066**	**14,801**	**14,788**

[77] Categories without corrections have not been replicated in the table.

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

VIC Police	Age of disclosure									
	0-3 months	3-6 months	6-9 months	9-12 months	12-15 months	15-18 months	18-21 months	21-24 months	Over 24 months	TOTAL (VIC Police)
18/19 Original	77,958	4,003	1,784	1,168	578	425	352	213	1,281	**87,762**
18/19 Updated[78]	79,751	4,654	1,984	1,476	820	255	352	413	1,464	**91,169**
19/20 Original	82,505	3,285	1,284	702	377	126	177	104	527	**89,087**
19/20 Updated[79]	82,900	6,570	3,935	1,225	1,056	461	323	497	1,498	**98,465**

[78] Corrections refer to Table 39, page 70, 2018–19 TIA Act Annual Report.
[79] Corrections refer to Table 38, page 72, 2019–20 TIA Act Annual Report.

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

VIC Police	Item 1: subscriber data	Items 2-6: traffic data	TOTAL (VIC Police)
18/19 Original	65,069	23,058	**88,127**
18/19 Updated[80]	67,548	23,621	**91,169**

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

VIC Police	Item 1: subscriber data	Items 2-6: traffic data	TOTAL (VIC Police)
19/20 Original	64,493	24,594	**89,087**
19/20 Updated[81]	71,025	27,440	**98,465**

[80] Corrections refer to Table 40, page 71, 2018–19 TIA Act Annual Report.
[81] Corrections refer to Table 39, page 73, 2019–20 TIA Act Annual Report.

Notes