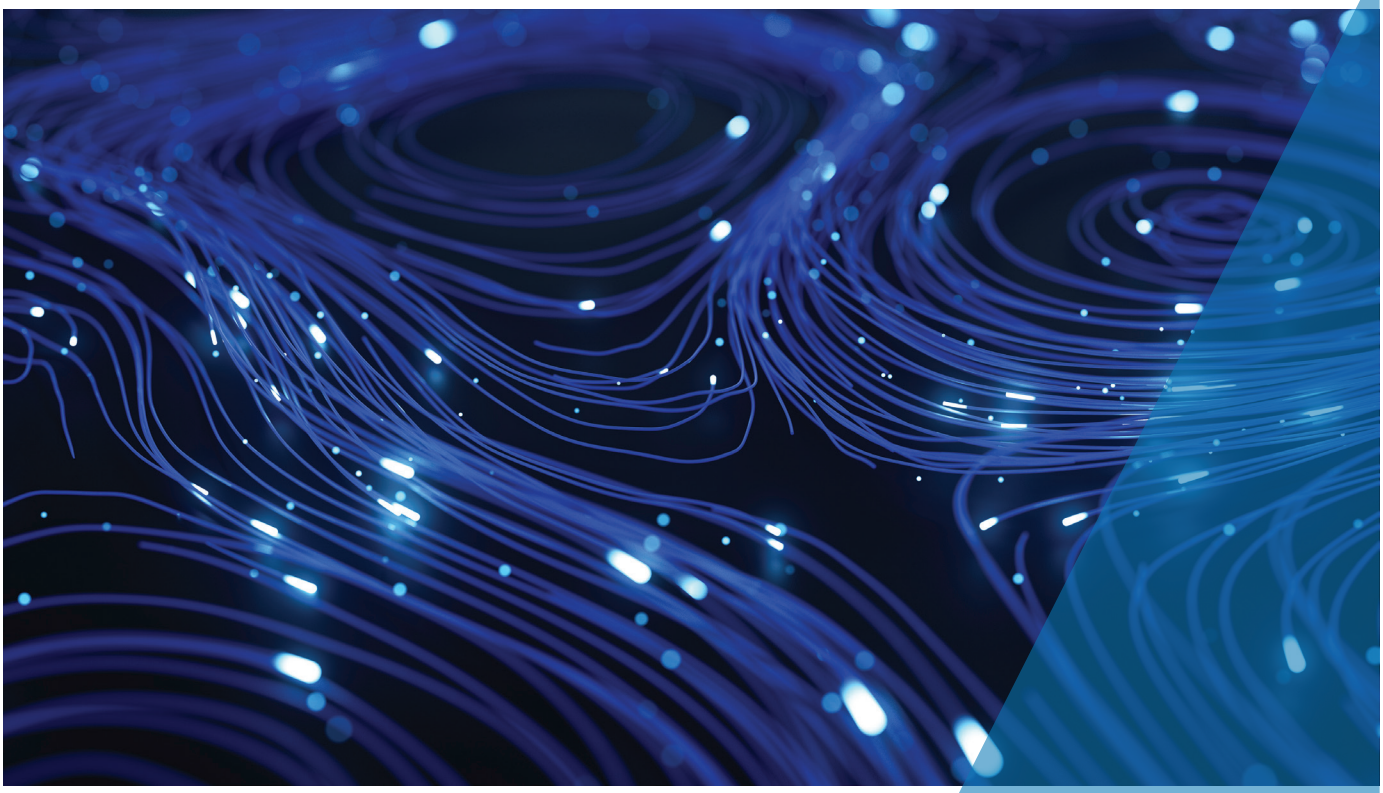
Australian Government
Department of Home Affairs



Telecommunications (Interception and Access) Act 1979

Annual Report 2020-21

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

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

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

Telecommunications (Interception and Access) Act 1979

Annual Report 2020–21

Contents

ABBREVIATIONS **1**

KEY STATISTICS **2**

CHAPTER 1 - INTRODUCTION **3**

Access to the content of a communication 3
Telecommunications data 4
Legislative reforms 4
Policy developments 5

CHAPTER 2 – TELECOMMUNICATIONS INTERCEPTION **7**

Serious offences 8
Eligibility to issue an interception warrant 11
Issuing of interception warrants 12
Applications for interception warrants 13
Warrants that authorise entry on to premises 15
Conditions or restrictions on warrants 15
Effectiveness of interception warrants 16
Named person warrants 21
B-Party warrants 25
Duration of warrants 27
Final renewals 28
Eligible warrants 29
Interception without a warrant 30
International assistance 30
Number of interceptions carried out on behalf of other agencies 30
Telecommunications interception expenditure 31
Emergency service facilities 33
Safeguards and reporting requirements on interception powers 34
Commonwealth Ombudsman – inspection of telecommunications interception records conducted in 2020-21 35

CHAPTER 3 – STORED COMMUNICATIONS **45**

Applications for stored communications warrants 45
Conditions or restrictions on stored communications warrants 48
Effectiveness of stored communications warrants 48
Preservation notices 49
International assistance 51
Ombudsman inspection report 52

CHAPTER 4 – TELECOMMUNICATIONS DATA **54**

Existing data – enforcement of the criminal law 55
Existing data – assist in locating a missing person 56
Existing data – enforcement of a law imposing a pecuniary penalty or protecting public revenue 57
Prospective data – authorisations 57
Data authorisations for foreign law enforcement 59
Offences for which authorisations were made 59
Age of data under disclosure 66
Types of retained data 68
Journalist information warrants 69
Industry estimated cost of implementing data retention 69

CHAPTER 5 – INDUSTRY ASSISTANCE **70**

Requests and notices 70
Use of industry assistance 72
Offences enforced through industry assistance 72
Oversight of industry assistance powers 73

CHAPTER 6 – FURTHER INFORMATION **75**

APPENDIX A – LISTS OF TABLES AND FIGURES **76**

APPENDIX B – INTERCEPTION AGENCIES UNDER THE TIA ACT **78**

APPENDIX C – CATEGORIES OF SERIOUS OFFENCES UNDER THE TIA ACT **79**

APPENDIX D – UPDATED FIGURES FOR PREVIOUS REPORTING PERIODS **80**

APPENDIX E – CATEGORIES OF OFFENCES ABBREVIATIONS **87**

APPENDIX F – RETAINED DATA SETS **88**

APPENDIX G – DESIGNATED COMMUNICATIONS PROVIDERS **92**

NOTES **94**

ABBREVIATIONS

Acronym	Agency/Organisation
AAT	Administrative Appeals Tribunal
ACIC	Australian Criminal Intelligence Commission
ACCC	Australian Competition and Consumer Commission
ACLEI	Australian Commission for Law Enforcement Integrity
AFP	Australian Federal Police
AGD	Attorney-General's Department
ASD	Australian Signals Directorate
ASIC	Australian Securities and Investments Commission
ASIO	Australian Security Intelligence Organisation
ASIS	Australian Secret Intelligence Service
Assistance and Access Act	*Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*
CCC (WA)	Corruption and Crime Commission (Western Australia)
Home Affairs	Department of Home Affairs
IBAC	Independent Broad-based Anti-corruption Commission (Victoria)
ICAC (NSW)	Independent Commission Against Corruption (New South Wales)
ICAC (SA)	Independent Commissioner Against Corruption (South Australia)
INSLM	Independent National Security Legislation Monitor
LECC	Law Enforcement Conduct Commission
NSW CC	New South Wales Crime Commission
NSW Police	New South Wales Police Force
NT Police	Northern Territory Police Force
PJCIS	Parliamentary Joint Committee on Intelligence and Security
QLD CCC	Queensland Corruption and Crime Commission
QLD Police	Queensland Police Service
SA Police	South Australia Police
TAN	Technical Assistance Notice
TAR	Technical Assistance Request
TAS Police	Tasmania Police
TCN	Technical Capability Notice
Telecommunications Act	*Telecommunications Act 1997*
TIA Act	*Telecommunications (Interception and Access) Act 1979*
VIC Police	Victoria Police
WA Police	Western Australia Police Force

KEY STATISTICS

The following key statistics are relevant to the 2020–21 reporting period.

- 3,481 interception warrants were issued to 16 interception agencies. This was a decrease of 196 on the 3,677 issued in 2019–20.
- The majority of serious offences that were specified in interception warrants issued were serious drug and trafficking offences (1,648 times specified), followed by loss of life or personal injury offences (614 times specified) and murder (405 times specified).
- Information obtained under interception warrants was used in 3,327 arrests, 6,424 prosecutions and 2,610 convictions.[1]
- 998 stored communications warrants were issued to 13 criminal law-enforcement agencies, a decrease of 396 on the 1,394 issued in 2019–20.
- 7 enforcement agencies made 470 arrests, conducted 740 proceedings, and obtained 376 convictions involving evidence obtained under stored communications warrants.
- 20 enforcement agencies made 317,403 authorisations for the disclosure of existing telecommunications data – an increase of 6,068 authorisations from the 311,335 authorisations made in 2019-20. Of these, 312,440 were made to enforce the criminal law.
- The majority of criminal law offences for which existing telecommunications data was requested were illicit drug offences (68,511 requests), followed by 28,964 requests for fraud and related offences and 27,385 requests for homicide offences.
- 39,289 authorisations were made by 19 criminal law-enforcement agencies for the disclosure of prospective telecommunications data, an increase of 6,355 on the 32,934 authorisations made in 2019-20.
- No Journalist Information Warrants were issued to enforcement agencies in 2020-21, a decrease from the 1 issued in 2019-20.
- Four interception agencies used powers under Part 15 of the *Telecommunications Act 1997* to request or require technical assistance from designated communications providers. 25 technical assistance requests were given by interception agencies, an increase of 14 from 2019-20. One technical assistance notice was given by NSW Police. This was the first technical assistance notice to be given to a designated communications provider since the commencement of the industry assistance framework.

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

CHAPTER 1 - INTRODUCTION

The 2020–21 Annual Report for the *Telecommunications (Interception and Access) Act 1979* (TIA 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 1997* between 1 July 2020 and 30 June 2021.

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

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

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

Access to the content of a communication

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

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

In some cases, the weight of this evidence results in defendants entering guilty pleas, thereby eliminating the need for the intercepted information to be introduced into evidence.

Telecommunications data

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

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

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

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

Amendments to the TIA Act in 2015, which introduced the mandatory data retention regime, reduced the number of enforcement agencies that could access telecommunications data under the TIA Act to 20 specified agencies. The Minister for Home Affairs may declare additional agencies in limited circumstances for a period of 40 sitting days of Parliament. No additional agencies were declared in the 2020–21 reporting period.

Legislative reforms

Telecommunications Legislation Amendment (International Production Orders) Act 2021

The *Telecommunications Legislation Amendment (International Production Orders) Act* 2021 (IPO Act) passed Parliament on 24 June 2021. The IPO Act amended the TIA Act to establish a new framework to assist Australia's international crime cooperation efforts by improving Australian agencies' access to overseas communications data for law enforcement and national security purposes. It provides the legislative framework for Australia to give effect to future international agreements for cross-border access to electronic information and communications data.

The framework introduced by the IPO Act and relevant agreements, is an alternative and complementary framework to other forms of international crime cooperation, mutual legal assistance and police-to-police cooperation.

The IPO Act can be found here: https://www.legislation.gov.au/Details/C2021A00078.

[2] Telecommunications data is information about a communication (such as the phone numbers of the people who called each other, how long they talked to each other, the email address from which a message was sent and the time the message was sent) or carriage services supplied (such as information about the identity of the subscriber) – but not the content of the communication.
[3] Existing data, also known as historical data, is information that is already in existence when an authorisation for disclosure is received by a telecommunications carrier.
[4] All 'criminal law-enforcement agencies' are set out in section 110A of the TIA Act. These agencies include all interception agencies as well as Home Affairs, ASIC, and the ACCC.
[5] Prospective data is telecommunications data that comes into existence during a period of time in which an authorisation is in force.

Policy developments

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

In July 2020, the then Independent National Security Legislation Monitor (INSLM), Dr James Renwick CSC SC, handed down his report concerning the new framework introduced by the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (Assistance and Access Act). The Assistance and Access Act introduced industry assistance measures in the *Telecommunications Act 1997* and computer access warrants in the *Surveillance Devices Act 2004* (SD Act) to better deal with the challenges posed by ubiquitous encryption. The INSLM was asked to consider whether the amendments introduced by the Assistance and Access Act contain appropriate safeguards for protecting the rights of individuals, and remains proportionate to the threats against national security and necessary.

The INSLM concluded that the amendments introduced by the Assistance and Access Act are necessary and proportionate, subject to some amendments that were recommended. The INSLM made 33 recommendations.

The INSLM report has been provided to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) to inform its current review of the Assistance and Access Act. The Department of Home Affairs made a submission to the PJCIS review which provided commentary on the INSLM's recommendations.

The Department's submission can be found here: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/AmendmentsTOLAAct2018/Submissions.

***Parliamentary Joint Committee on Intelligence and Security review of the amendments made by the* Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018**

At the end of the reporting period, the PJCIS was still conducting its third review into the Assistance and Access Act. This review builds on both the previous two PJCIS reviews, and the INSLM review of the Assistance and Access Act.

The Government will carefully consider the findings made by the INSLM and PJCIS review together.

Further information on this review can be found here: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/AmendmentsTOLAAct2018.

Comprehensive Review of the legal framework of the National Intelligence Community

The current electronic surveillance legislative framework was examined in detail by the Comprehensive Review of the Legal Framework of the National Intelligence Community (Comprehensive Review). The Comprehensive Review identified that the current laws are complex, inconsistent, outdated and inflexible. Frequent amendments to the legislation are needed to keep pace with technological change and the evolving criminal and national security threats resulting in a patchwork of overlapping and at times inconsistent or incompatible parts. This puts at risk the effectiveness of protections for people's information and data, and the proper governance of agencies who access this information. It also creates difficulties for agencies when investigating serious criminality and threats to national security.

In its response to the Comprehensive Review, the Government committed to reform the existing laws and develop a new Act that is clearer, more coherent and better adapted to the modern world. On 1 July 2021, the Department of Home Affairs established an interagency taskforce to deliver on the Government's commitment. This will involve repealing and replacing the powers currently divided between the TIA Act, the SD Act and relevant parts of the *Australian Security Intelligence Organisation Act 1979* into one consolidated Act.

The development of a new electronic surveillance legislative framework will require detailed consideration, informed by extensive consultation with Commonwealth, State and Territory government agencies, international partners, industry, civil society groups and the public. The Government intends to develop a new modernised and streamlined electronic surveillance legislative framework by 2023.

The Government will conduct open and iterative public consultation throughout the development of the new framework.

Further information can be found here: https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/electronic-surveillance-reform

CHAPTER 2 – TELECOMMUNICATIONS INTERCEPTION

The interception of communications is regulated by Chapter 2 of the TIA Act. The primary function of Chapter 2 of the TIA Act is to prohibit communications from being intercepted while they are passing over an Australian telecommunications system, except as authorised under the circumstances set out in the TIA Act. This protects the privacy of the communications of people who use the Australian telecommunications network.

Definition

The term **'interception agency'** is defined in section 5 of the TIA Act. An interception agency is limited to bodies such as the AFP, 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 access to real-time content (for example, a live phone call between two parties). During the reporting period, interception warrants were available to 17 Commonwealth, State and Territory agencies including:

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

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

Definition

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

Serious offences

Interception warrants can be obtained to investigate serious offences as set out in section 5D of the TIA Act. Serious offences generally carry a penalty of at least seven years' imprisonment.[6]

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

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

This information is presented in Table 1. This table illustrates the important role telecommunications interception plays in investigating serious offences. Consistent with previous years, in 2020–21 the majority of warrants obtained were to assist with investigations into serious drug offences and/or trafficking (1,648 warrants). Loss of life or personal injury offences were specified in 614 warrants and 405 related to murder investigations. Money laundering was specified as an offence in 178 warrants. The total number of offences is typically larger than the total number of warrants issued, as a warrant can be issued to investigate more than one serious offence.

Information about offences covered under each category is set out in Appendix C.

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

Table 1: Categories of serious offences specified in interception warrants – paragraphs 100(1)(f), 100(1)(g), 100(2)(f) and 100(2)(g)

Categories of offences	ACIC	AFP	CCC (WA)	IBAC	ICAC (NSW)	ICAC (SA)	LECC	NT Police	NSW CC	NSW Police	QLD CCC	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Administration of justice / government offences	-	16	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**16**
Assisting person to escape or dispose of proceeds	-	-	-	-	-	-	-	-	9	1	-	6	-	-	3	-	**19**
Bribery, corruption and dishonesty offences	-	18	31	10	11	8	24	2	-	17	22	-	3	-	3	2	**151**
Cartel offences	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**1**
Child abuse offences	-	5	-	-	-	-	2	-	-	1	-	-	-	-	-	1	**9**
Conspire/aid/abet serious offence	-	-	-	-	-	2	-	1	5	6	-	-	-	-	1	-	**15**
Cybercrime offences	-	5	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**5**
Espionage and foreign interference	-	9	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**9**
Kidnapping	-	8	-	-	-	-	-	-	-	60	-	-	6	-	3	-	**77**
Loss of life or personal injury	-	38	-	-	-	-	-	1	-	448	-	39	1	-	37	50	**614**
Money laundering	-	112	-	-	-	-	-	1	15	8	6	9	7	-	-	20	**178**
Murder	-	24	-	-	-	-	-	4	8	228	-	49	7	4	36	45	**405**
Offences involving planning and organisation	-	2	-	-	-	-	-	5	-	106	-	5	-	-	4	17	**139**

Categories of offences	ACIC	AFP	CCC (WA)	IBAC	ICAC (NSW)	ICAC (SA)	LECC	NT Police	NSW CC	NSW Police	QLD CCC	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Organised offences and/or criminal organisations	-	-	-	-	-	-	-	-	-	29	-	-	-	-	-	-	**29**
People smuggling and related	-	4	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**4**
Serious damage to property and/or serious arson	-	7	-	-	-	-	-	1	-	27	-	1	-	-	1	6	**43**
Serious drug offences and/or trafficking	-	407	-	-	-	-	-	17	70	756	11	147	18	5	46	171	**1,648**
Serious fraud	-	52	-	-	-	-	-	-	-	79	8	-	-	-	-	15	**154**
Serious loss of revenue	-	23	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**23**
Special ACC investigations	72	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**72**
Terrorism financing offences	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**1**
Terrorism offences	-	57	-	-	-	-	-	-	-	-	-	-	-	-	1	-	**58**
TOTAL	**72**	**789**	**31**	**10**	**11**	**10**	**26**	**32**	**107**	**1,766**	**47**	**256**	**42**	**9**	**135**	**327**	**3,670**

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;
- Family Court of Australia; and
- Federal Circuit Court.

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

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

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 Tables 2 and 3. In 2020–21 there were 93 issuing authorities for interception warrants.

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

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

Issuing of interception warrants

Table 3 states which authorities considered applications for warrants made by each interception agency during 2020–21. In 2020-21, nominated AAT members considered 83 percent of total interception warrant applications made.

Table 3: Number of interception warrant applications considered by Federal Court judges, Family Court judges, Federal Circuit Court judges and nominated AAT members – paragraph 103(ab)

Agency	Issuing Authority				
	Family Court judges	Federal Circuit Court judges	Federal Court judges	Nominated AAT members	TOTAL
ACIC	5	-	11	56	**72**
AFP	1	55	7	590	**653**
CCC (WA)	31	-	-	-	**31**
IBAC	-	-	-	12	**12**
ICAC (NSW)	-	-	-	11	**11**
ICAC (SA)	-	-	-	10	**10**
LECC	-	-	-	26	**26**
NT Police	-	31	-	1	**32**
NSW CC	-	-	-	97	**97**
NSW Police	-	-	72	1,683	**1,755**
QLD CCC	-	20	-	11	**31**
QLD Police	-	205	-	44	**249**
SA Police	-	-	-	34	**34**
TAS Police	-	-	-	9	**9**
VIC Police	-	-	-	139	**139**
WA Police	144	-	-	183	**327**
TOTAL	**181**	**311**	**90**	**2,906**	**3,488**

Applications for interception warrants

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

Table 4 presents this information. In 2020–21 agencies were issued 3,481 interception warrants, a decrease of 196 from 2019–20, where 3,677 warrants were issued. 752 renewals of interception warrants were issued in 2020–21. This represents an increase of 15 from the previous reporting period. There was a decrease in the number of telephone applications from 42 to 4.

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

Agency	Relevant Statistics	Applications for warrants		Telephone applications for warrants		Renewal applications	
		19/20	20/21	19/20	20/21	19/20	20/21
ACIC	Made	109	72	2	-	23	23
	Refused	-	-	-	-	-	-
	Issued	109	72	2	-	23	23
ACLEI	Made	3	-	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	3	-	-	-	-	-
AFP	Made	638	653	-	-	229	199
	Refused	2	-	-	-	-	-
	Issued	636	653	-	-	229	199
CCC (WA)	Made	41	31	-	-	11	12
	Refused	-	-	-	-	-	-
	Issued	41	31	-	-	11	12
IBAC	Made	26	12	-	-	2	5
	Refused	2	2	-	-	-	-
	Issued	24	10	-	-	2	5
ICAC (NSW)	Made	7	11	-	-	-	2
	Refused	-	-	-	-	-	-
	Issued	7	11	-	-	-	2
ICAC (SA)	Made	23	10	-	-	11	1
	Refused	-	-	-	-	-	-
	Issued	23	10	-	-	11	1
LECC	Made	14	26	-	-	6	10
	Refused	-	-	-	-	-	-

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

Agency	Relevant Statistics	Applications for warrants		Telephone applications for warrants		Renewal applications	
		19/20	20/21	19/20	20/21	19/20	20/21
	Issued	14	26	-	-	6	10
NT Police	Made	18	32	-	-	-	1
	Refused	-	-	-	-	-	-
	Issued	18	32	-	-	-	1
NSW CC	Made	144	97	-	-	34	34
	Refused	-	-	-	-	-	-
	Issued	144	97	-	-	34	34
NSW Police	Made	1,860	1,755	39	2	330	379
	Refused	-	-	-	-	-	-
	Issued	1,860	1,755	39	2	330	379
QLD CCC	Made	27	31	-	-	6	3
	Refused	-	-	-	-	-	-
	Issued	27	31	-	-	6	3
QLD Police	Made	256	249	-	-	44	42
	Refused	-	1	-	-	-	-
	Issued	256	248	-	-	44	42
SA Police	Made	36	34	1	-	3	2
	Refused	-	-	-	-	-	-
	Issued	36	34	1	-	3	2
TAS Police	Made	13	9	-	-	1	1
	Refused	-	-	-	-	-	-
	Issued	13	9	-	-	1	1
VIC Police	Made	146	139	-	2	17	11
	Refused	3	4	-	-	-	-
	Issued	143	135	-	2	17	11
WA Police	Made	323	327	-	-	20	27
	Refused	-	-	-	-	-	-
	Issued	323	327	-	-	20	27
TOTAL	**Made**	**3,684**	**3,488**	**42**	**4**	**737**	**752**
	Refused	**7**	**7**	**0**	**0**	**0**	**0**
	Issued	**3,677**	**3,481**	**42**	**4**	**737**	**752**

Warrants that authorise entry on to premises

The TIA Act provides that an issuing authority can issue an interception warrant that authorises entry on to premises. An issuing authority can only issue such a warrant if satisfied that it would be impracticable or inappropriate to intercept communications otherwise than by use of equipment installed on those premises. Agencies do not typically apply for this type of warrant.

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

In 2020–21, no agencies applied for interception warrants that authorised entry on premises. This has not changed from 2019-20.

Conditions or restrictions on warrants

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

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

Table 5 presents this information. In 2020-21, 64 interception warrants were issued with a condition or restriction, a decrease of 43 compared to the 107 issued in the 2019–20 reporting period.

Table 5: 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	
	19/20	20/21
AFP	4	1
ICAC NSW	1	-
LECC	-	4
NT Police	-	2
NSW CC	4	1
NSW Police	80	56
QLD CCC	13	-
SA Police	2	-
WA Police	3	-
TOTAL	**107**	**64**

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 their lawfully intercepted information culminated in an arrest by another agency. This removes the risk that arrest numbers will be duplicated due to multiple agencies reporting on the same arrest. This also shows the outcomes from agencies that do not have arrest powers themselves but whose lawfully intercepted information ultimately leads to an arrest by another agency.

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

Tables 6, 7 and 8 provide this information. In 2020–21 there were 3,327 arrests made as a result of lawfully intercepted information. There were also 6,424 prosecutions and 2,610 convictions where lawfully intercepted material was given in evidence.

The information provided in this section should be interpreted with some caution, particularly in presuming a relationship between the number of arrests, prosecutions (which include committal proceedings) and convictions in a reporting period. An arrest recorded in one reporting period may not result in a prosecution until a later reporting period. Any resulting conviction could be recorded in that, or a subsequent reporting

period. Additionally, one arrest may be prosecuted and convicted for a number of offences, some or all of which may be prosecuted at a later time.

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

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

Agency	19/20		20/21	
	Number of arrests by agency	Number of times lawfully intercepted information culminated in arrest by another agency	Number of arrests by agency	Number of times lawfully intercepted information culminated in arrest by another agency
ACIC	-	17	-	27
AFP	137	54	132	44
ICAC (SA)	-	5	-	1
LECC	-	-	-	1
NT Police	18	9	25	14
NSW CC	-	69	-	107
NSW Police	1,378	5	1,478	13
QLD CCC	8	-	20	14
QLD Police	390	-	316	-
SA Police	34	-	53	-
TAS Police	1	10	17	-
VIC Police	289	42	269	42
WA Police	430	364	407	347
TOTAL	**2,685**	**575**	**2,717**	**610**

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

Category	AFP	IBAC	ICAC (SA)	NT Police	NSW CC	NSW Police	QLD CCC	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Administration of justice / government offences	1	-	-	-	-	-	-	-	-	-	-	-	**1**
Assisting person to escape or dispose of proceeds	-	-	-	-	-	-	-	-	-	-	2	-	**2**
Bribery or corruption	-	2	-	-	-	1	3	-	-	-	-	6	**12**
Child abuse offences	-	-	-	-	-	2	-	-	-	-	-	6	**8**
Conspire/aid/abet serious offence	-	-	2	-	-	-	-	-	-	-	1	6	**9**
Cybercrime offences	-	-	-	-	-	125	-	-	-	-	-	-	**125**
Kidnapping	-	-	-	-	-	19	-	-	-	-	-	-	**19**
Loss of life	1	-	-	-	-	2	-	-	-	-	2	8	**13**
Money laundering	16	-	-	1	2	270	-	-	-	-	6	49	**344**
Murder	-	-	-	-	1	46	-	-	6	-	13	12	**78**
Offences involving planning and organisation	6	-	-	-	-	75	-	-	-	-	16	127	**224**
Organised crime	-	-	-	-	1	19	-	-	-	-	-	-	**20**
Other offence punishable by 3 years to life	6	-	3	-	-	78	12	64	-	-	57	-	**220**
Serious arson	-	-	-	-	-	17	-	-	-	-	2	4	**23**
Serious damage to property	-	-	-	-	-	2	-	-	-	-	-	12	**14**
Serious drug offence and/or trafficking	72	-	-	23	16	3,042	2	72	1	17	117	1,487	**4,849**
Serious fraud	-	1	-	1	-	69	4	5	-	-	16	5	**101**
Serious personal injury	-	-	-	-	-	300	-	-	-	-	27	24	**351**

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

Category	AFP	IBAC	ICAC (SA)	NT Police	NSW CC	NSW Police	QLD CCC	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Telecommunications offences	3	-	-	-	-	5	-	-	-	-	-	-	**8**
Terrorism offences	3	-	-	-	-	-	-	-	-	-	-	-	**3**
Total	**108**	**3**	**5**	**25**	**20**	**4,072**	**21**	**141**	**7**	**17**	**259**	**1,746**	**6,424**

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

Category	AFP	IBAC	ICAC (SA)	NT Police	NSW CC	NSW Police	QLD CCC	QLD Police	SA Police	VIC Police	WA Police	TOTAL
Administration of justice / government offences	6	-	-	-	-	-	-	-	-	-	-	**6**
Assisting person to escape or dispose of proceeds	-	-	-	-	-	-	-	-	-	2	-	**2**
Bribery or corruption	-	2	-	-	-	-	-	-	-	-	2	**4**
Child abuse offences	-	-	-	-	-	1	-	-	-	-	2	**3**
Conspire/aid/abet serious offence	5	-	2	-	-	-	-	-	-	1	2	**10**
Kidnapping	-	-	-	-	-	7	-	-	-	-	-	**7**
Loss of life	1	-	-	-	-	1	-	-	-	2	3	**7**
Money laundering	7	-	-	-	2	5		-	1	6	12	**33**
Murder	-	-	-	-	1	14	-	-	5	6	5	**31**

Offences involving planning and organisation	-	-	-	-	-	33	-	-	-	16	69	**118**
Organised crime	-	-	-	-	1	16	-	-	-	-	-	**17**
Other offence punishable by three years to life	5	-	3	-	-	24	8	64	-	39	-	**143**
Serious arson	-	-	-	-	-	17	-	-	-	-	2	**19**
Serious damage to property	-	-	-	-	-	1	-	-	-	-	5	**6**
Serious drug offence and/or trafficking	39	-	-	2	11	650	2	63	35	93	1,135	**2,030**
Serious fraud	-	1	-	-	-	18	4	5	-	10	2	**40**
Serious personal injury	-	-	-	-	-	97	-	-	-	16	12	**125**
Telecommunications offences	-	-	-	-	-	5	-	-	-	-	-	**5**
Terrorism offences	4	-	-	-	-	-	-	-	-	-	-	**4**
Total	**67**	**3**	**5**	**2**	**15**	**889**	**14**	**132**	**41**	**191**	**1,251**	**2,610**

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;
- whether the interception will assist in the investigation; and
- the extent to which methods other than using a named person warrant are available to the agency.

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

Tables 9 and 10 present this information. In 2020–21, 553 named person warrants were issued, a decrease of 88 from the 2019–20 reporting period in which 641 named person warrants were issued. There was also a decrease of 33 in the number of renewal applications from 184 in 2019-20 to 151 in 2020-21.

Table 9: Original applications for named person warrants, telephone applications for named person warrants, and renewal applications – paragraphs 100(1)(ea) and 100(2)(ea)[8]

Agency	Relevant Statistics	Applications for named person warrants		Telephone applications for named person warrants		Renewal applications for named person warrants	
		19/20	20/21	19/20	20/21	19/20	20/21
ACIC	Made	54	39	2	-	17	13
	Refused	-	-	-	-	-	-
	Issued	54	39	2	-	17	13
AFP	Made	224	196	-	-	97	63
	Refused	-	-	-	-	-	-
	Issued	224	196	-	-	97	63
CCC (WA)	Made	3	3	-	-	1	-
	Refused	-	-	-	-	-	-
	Issued	3	3	-	-	1	-
IBAC	Made	1	6	-	-	-	3
	Refused	-	-	-	-	-	-

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

Agency	Relevant Statistics	Applications for named person warrants		Telephone applications for named person warrants		Renewal applications for named person warrants	
		19/20	20/21	19/20	20/21	19/20	20/21
LECC	Issued	1	6	-	-	-	3
	Made	4	6	-	-	-	5
	Refused	-	-	-	-	-	-
	Issued	4	6	-	-	-	5
NT Police	Made	-	1	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	-	1	-	-	-	-
NSW CC	Made	52	46	-	-	16	13
	Refused	-	-	-	-	-	-
	Issued	52	46	-	-	16	13
NSW Police	Made	121	93	-	-	31	34
	Refused	-	-	-	-	-	-
	Issued	121	93	-	-	31	34
QLD CCC	Made	-	3	-	-	-	2
	Refused	-	-	-	-	-	-
	Issued	-	3	-	-	-	2
QLD Police	Made	43	31	-	-	4	5
	Refused	-	-	-	-	-	-
	Issued	43	31	-	-	4	5
SA Police	Made	2	4	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	2	4	-	-	-	-
TAS Police	Made	1	2	-	-	1	-
	Refused	-	-	-	-	-	-
	Issued	1	2	-	-	1	-
VIC Police	Made	57	35	-	-	11	4
	Refused	1	1	-	-	-	-
	Issued	56	34	-	-	11	4
WA Police	Made	80	69	-	-	6	9
	Refused	-	-	-	-	-	-
	Issued	80	69	-	-	6	9
TOTAL	**Made**	**642**	**534**	**2**	**0**	**184**	**151**
	Refused / Withdrawn	**1**	**1**	**0**	**0**	**0**	**0**
	Issued	**641**	**533**	**2**	**0**	**184**	**151**

In 2020–21, 11 named person warrants were issued with a condition or restriction. This is an increase of two compared to the nine issued with a condition or restriction in the 2019–20 period.

Table 10: 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	
	19/20	20/21
AFP	-	1
LECC	-	4
NSW CC	3	1
NSW Police	6	2
QLD CCC	-	3
TOTAL	**9**	**11**

Paragraphs 100(1)(eb) and 100(2)(eb) of the TIA Act provide that this report must set out, in relation to all named person warrants issued during the year on applications made by each agency, the number of services intercepted in the categories outlined in Table 11. Consistent with previous reporting periods, in 2020–21 the majority of named person warrants related to two to five telecommunications services.

Table 11: Number of 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	
	19/20	20/21	19/20	20/21	19/20	20/21	19/20	20/21
ACIC	23	12	25	26	5	1	-	-
AFP	92	85	116	97	8	6	5	5
CCC (WA)	1	2	1	1	-	-	1	-
IBAC	-	-	1	6	-	-	-	-
LECC	-	1	3	4	1	1	-	-
NT Police	-	-	-	1	-	-	-	-
NSW CC	26	20	25	26	1	-	-	-
NSW Police	48	32	69	58	4	3	-	-
QLD CCC	-	-	-	-	-	3	-	-
QLD Police	10	8	28	20	4	3	1	-
SA Police	1	1	1	3	-	-	-	-
TAS Police	-	-	1	1	-	1	-	-
VIC Police	20	14	23	20	2	-	-	-
WA Police	26	22	52	45	-	2	-	-
TOTAL	**247**	**197**	**345**	**308**	**25**	**20**	**7**	**5**

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

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

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

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

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

Tables 12 and 13 outline the number of services and devices intercepted under the different types of named person warrants.

Table 12: Total number of services intercepted under service-based named person warrants – paragraphs 100(1)(ec) and 100(2)(ec)

Agency	Services	
	19/20	20/21
ACIC	47	60
AFP	528	427
CCC WA	38	4
IBAC	3	20
LECC	17	18
NSW CC	98	46
NSW Police	114	205
NT Police	-	1
QLD CCC	-	6
QLD Police	144	77
SA Police	2	7
TAS Police	3	9
VIC Police	99	67
WA Police	152	141
TOTAL	**1,245**	**1,088**

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

Agency	Devices		Services	
	19/20	20/21	19/20	20/21
ACIC	21	24	17	26
AFP	61	94	304	51
NSW CC	-	-	3	-
NSW Police	15	14	19	38
VIC Police	11	-	-	-
WA Police	2	6	-	-
TOTAL	**110**	**138**	**343**	**115**

B-Party warrants

Definition

A **'B-Party warrant'** is a telecommunications service warrant that enables an interception agency to intercept the communications of a person who is communicating with a person suspected of involvement in a serious offence.

An issuing authority can issue a B-Party warrant, but only if there are no other practicable methods of identifying the telecommunications services of the person involved in the offences, or if the interception of communications from that person's telecommunications services would not otherwise be possible.

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

This information is presented in Tables 14 and 15. In 2020–21, 54 B-Party warrants were issued to interception agencies. This represents a decrease of 44 from the 98 B-Party warrants issued in 2019–20.

Table 14: Applications for B-Party warrants, telephone applications and renewal applications for B-Party warrants– paragraphs 100(1)(ed) and 100(2)(ed)[9]

Agency	Relevant Statistics	Applications for B-Party Warrants		Telephone applications for B-Party warrants		Renewal applications for B-Party warrants	
		19/20	20/21	19/20	20/21	19/20	20/21
ACIC	Made	2	1	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	2	1	-	-	-	-
AFP	Made	31	17	-	-	17	10
	Refused	-	-	-	-	-	-
	Issued	31	17	-	-	17	10
NSW CC	Made	3	-	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	3	-	-	-	-	-
NSW Police	Made	60	36	13	2	3	-
	Refused	-	-	-	-	-	-
	Issued	60	36	13	2	3	-
SA Police	Made	1	-	1	-	-	-
	Refused	-	-	-	-	-	-
	Issued	1	-	1	-	-	-
WA Police	Made	1	-	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	1	-	-	-	-	-
TOTAL	**Made**	**98**	**54**	**14**	**2**	**20**	**10**
	Refused	**0**	**0**	**0**	**0**	**0**	**0**
	Issued	**98**	**54**	**14**	**2**	**20**	**10**

In 2020–21, three B-Party warrants were issued with conditions or restrictions. This is a decrease from seven in the 2019–20 reporting period.

Table 15: B-Party warrants issued with conditions or restrictions – paragraphs 100(1)(ed) and 100(2)(ed)

Agency	B-party warrants specifying conditions or restrictions	
	19/20	20/21
NSW Police	6	3
WA Police	1	-
TOTAL	**7**	**3**

[9] 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.

In 2020-21, no B-Party warrants issued on applications made by an agency authorised entry onto premises.

Duration of warrants

Under the TIA Act, an interception warrant, other than a B-Party warrant, can be in force for up to 90 days. Under section 57, the chief officer of an agency may revoke a warrant at any time and must revoke a warrant if they are satisfied that the grounds on which the warrant was issued no longer exist.

Paragraphs 101(1)(a)-(d) and 101(2)(a)-(d) of the TIA Act provide that this report must set out for each agency the average length of time for which interception warrants – including renewals, but not including B-Party warrants – were issued, and the average length of time they were in force in the reporting period.

Table 16: 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)[10]	Average period specified in warrants (days)	Average period warrants in force (days)[11]
ACIC	88	73	90	80
AFP	79	61	83	73
CCC (WA)	90	59	90	42
IBAC	73	73	72	72
ICAC (NSW)	83	79	68	68
ICAC (SA)	72	70	90	90
LECC	79	66	90	79
NT Police	89	88	-	-
NSW CC	84	71	84	67
NSW Police	62	48	75	57
QLD CCC	60	54	89	88
QLD Police	79	63	70	53
SA Police	75	53	90	46
TAS Police	90	59	90	-
VIC Police	85	63	81	55
WA Police	85	56	87	68
AVERAGE	**72**	**55**	**79**	**63**

[10] This column excludes warrants that did not cease before the end of the reporting period.
[11] 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 102(2)(da) of the TIA Act provide that this report must set out for each agency the average length of time for which B-Party warrants – including renewals – were specified to be in force when issued, and the average length of time they were actually in force during the reporting period.

Table 17: Duration of original and renewal B-Party warrants – paragraphs 101(1)(da) and 102(2)(da)

Agency	Duration of original telecommunications B-party warrants		Duration of renewal telecommunications B-party warrants	
	Average period specified in warrants (days)	Average period warrants in force (days)	Average period specified in warrants (days)	Average period warrants in force (days)
ACIC	45	45	-	-
AFP	45	45	45	45
NSW Police	28	13	-	-
AVERAGE	**34**	**24**	**45**	**45**

Final renewals

A final renewal means an interception warrant that is the last renewal of an original warrant. A final renewal is recorded as the number of days after the issue of the original warrant. Paragraphs 101(1)(e) and 101(2)(e) of the TIA Act provide that this report must set out how many final renewals ceased to be in force during that year. The categories of final renewals are:

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

Table 18 presents information on the number of final renewals of warrants by agencies.

Table 18: Number of final renewals – paragraphs 101(1)(e) and 101(2)(e)

Agency	90 days		150 days		180 days	
	19/20	20/21	19/20	20/21	19/20	20/21
ACIC	6	10	3	0	3	3
AFP	4	5	12	39	39	46
CCC (WA)	-	9	11	3	-	-
IBAC	-	4	-	3	-	-
ICAC (NSW)	-	2	-	-	-	-
LECC	1	-	1	7	4	1
NSW CC	7	4	1	4	1	5
NSW Police	118	122	28	36	50	63

Agency	90 days		150 days		180 days	
	19/20	20/21	19/20	20/21	19/20	20/21
QLD CCC	-	-	2	-	2	-
QLD Police	15	23	17	11	7	1
SA Police	-	4	1	-	-	-
TAS Police	1	-	-	-	-	-
VIC Police	5	8	4	3	-	-
WA Police	6	13	3	18	3	-
TOTAL	**163**	**204**	**83**	**124**	**109**	**119**

Eligible warrants

Definition

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

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

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

Table 19 presents this information. In 2020–21, 69 per cent of total warrants were eligible warrants.

Table 19: Percentage of eligible warrants – paragraphs 102(3) and 102(4)[12]

Agency	Number of eligible warrants	Total number of warrants in force	%
ACIC	56	91	62%
AFP	376	768	49%
CCC (WA)	23	45	51%
IBAC	12	18	67%
ICAC (NSW)	15	17	88%
ICAC (SA)	2	18	11%
LECC	4	31	13%
NT Police	17	36	47%
NSW CC	54	134	40%
NSW Police	1,740	2,093	83%
QLD CCC	9	33	27%
QLD Police	271	287	94%

[12] 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 more recent reporting period.

Agency	Number of eligible warrants	Total number of warrants in force	%
SA Police	31	41	76%
TAS Police	4	9	44%
VIC Police	79	164	48%
WA Police	176	398	44%
TOTAL	**2,869**	**4,183**	**69%**

Interception without a warrant

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

In 2020–21, there were no instances where agencies intercepted communications under subsections 7(4) or (5) of the TIA Act without a warrant. There was no change from 2019-20.

International assistance

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

- a foreign country under sections paragraph 68(l) or section 68A of the TIA Act in connection with an authorisation under section 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*;
- 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 2020–21, there were no occasions in which lawfully intercepted information or interception warrant information was provided to a foreign country under international assistance. There was no change from 2019-20.

Number of interceptions carried out on behalf of other agencies

The TIA Act supports the ability of interception agencies to cooperate and to work collaboratively by enabling one interception agency to carry out interception on behalf of other 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 20: Number of interceptions carried out on behalf of other agencies – paragraph 103(ac)

Interception carried out by:	Interception carried out on behalf of:	Number of interceptions
ACIC	QLD CCC	31
CCC WA	ICAC (SA)	10
VIC Police	TAS Police	8
TOTAL		**49**

Telecommunications interception expenditure

Table 21 provides information about the total expenditure (including expenditure of a capital nature) by interception agencies on interception warrants and the average expenditure per warrant (total warrant expenditure divided by the number of warrants issued) per warrant. The average cost per warrant is significantly affected by capital expenditure (which can vary significantly, for instance, due to a capital upgrade program) and the number of warrants issued, meaning that smaller interception agencies typically have higher average costs as they apply for fewer warrants.

Care should be taken in comparing costs associated with average expenditure as interception agencies employ different interception models which may result in some costs associated with interception being delineated, and for other agencies, those same costs being included in their average expenditure.

Table 21: Total expenditure incurred by each agency in connection with the execution of interception warrants and average expenditure per interception warrant – paragraphs 103(a) and 103(aa)

Agency	Total expenditure	Average expenditure
ACIC	$5,339,535	$74,160
AFP	$20,882,301	$31,979
CCC (WA)	$656,786	$21,187
IBAC	$703,303	$70,330
ICAC (NSW)	$472,202	$42,927
ICAC (SA)	$138,452	$13,845
LECC	$906,439	$34,863
NT Police	$1,108,794	$34,649
NSW CC	$1,578,777	$16,276
NSW Police	$10,187,096	$5,804
QLD CCC	$1,642,846	$52,995
QLD Police	$11,157,453	$44,989
SA Police	$4,232,302	$124,479
TAS Police	$951,807	$105,756
VIC Police	$663,109	$4,912
WA Police	$4,091,550	$12,512
TOTAL / AVERAGE	**$64,712,752**	**$18,590**

Table 22 provides a breakdown of the total recurrent costs of interception over the reporting period. As agencies do not necessarily treat or record particular items of expenditure in the same way, caution should be exercised in comparing costs incurred by individual agencies.

Table 22: Recurrent interception costs per agency

Agency	Salaries	Administrative Support	Capital expenditure	Interception costs	Total ($)
ACIC	$3,687,722	$378,592	$73,169	$1,200,052	**$5,339,535**
ACLEI	$86,080	$1,962	-	-	**$88,042**
AFP	$8,241,072	$191,826	-	$12,449,403	**$20,882,301**
CCC (WA)	$317,085	$10,000	$241,400	$88,301	**$656,786**
IBAC	$519,640	$6,242	$74,460	$102,961	**$703,303**
ICAC (NSW)	$279,054	-	-	$193,148	**$472,202**
ICAC (SA)	$72,720	$64,092	-	$1,640	**$138,452**
LECC	$636,805	$2,590	$81,441	$185,603	**$906,439**

Agency	Salaries	Administrative Support	Capital expenditure	Interception costs	Total ($)
NT Police	$839,950	$174,856	$83,418	$10,570	**$1,108,794**
NSW CC	$1,040,454	$48,961	-	$489,362	**$1,578,777**
NSW Police	$7,280,538	$520,731	-	$2,385,827	**$10,187,096**
QLD CCC	$1,093,856	$192,443	-	$356,547	**$1,642,846**
QLD Police	$4,813,742	$785,398	$3,825,952	$1,732,361	**$11,157,453**
SA Police	$2,717,343	$142,196	$498,532	$874,231	**$4,232,302**
TAS Police	$778,782	$6,797	$2,907	$163,321	**$951,807**
VIC Police	$513,834	$4,801	$45,642	$68,832	**$633,109**
WA Police	$3,568,446	$248,004	-	$275,100	**$4,091,550**
TOTAL	**$36,487,123**	**$2,779,491**	**$4,926,921**	**$20,578,975**	**$64,772,510**

Emergency service facilities

Under the TIA Act, listening to or recording calls to and from a facility declared by the Minister for Home Affairs to be an emergency service facility is not interception. This exemption ensures that emergency services can assist emergency callers and respond to critical situations as quickly as possible, without the need to first obtain a caller's consent to the recording of the call. Table 23 sets out the number of places that have been declared under the TIA Act during the reporting period to be emergency service facilities.

Table 23: Emergency service facility declarations – paragraph 103(ad)

Agency	Police	Fire brigade	Ambulance	Despatching
New South Wales	7	82	6	7
Victoria	-	-	-	1
TOTAL	**7**	**82**	**6**	**8**

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

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

At least twice a year the Commonwealth Ombudsman must inspect the records kept by the ACIC, the ACLEI, and the AFP relating to interceptions, and the use, dissemination and destruction of intercepted information. The inspections are retrospective, and for this reason, the Ombudsman inspected relevant telecommunications interception warrants that were expired or revoked in the period between 1 January and 31 December 2020.

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

While the Commonwealth Ombudsman is responsible for inspecting the records of the ACIC, the ACLEI, and the AFP in relation to interception, the relevant State or Territory Ombudsman generally undertakes this function for State and Territory agencies. The reports of the inspections of the declared State and Territory agencies are given to the responsible State or Territory minister who provides a copy to the Commonwealth Minister for Home Affairs. The Commonwealth Ombudsman also conducts inspections of records in relation to access by enforcement agencies (including both Commonwealth and State agencies) to stored communications and telecommunications data.

Commonwealth Ombudsman – inspection of telecommunications interception records conducted in 2020-21

Overview

During 2020-21, the Commonwealth Ombudsman (the Ombudsman) conducted 5 inspections under s 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 30 June 2020 and 1 July and 31 December 2020, and consisted of:

- two inspections at the Australian Federal Police (AFP)
- two inspections at the Australian Criminal Intelligence Commission (ACIC), and
- one inspection at the Australian Commission for Law Enforcement Integrity (ACLEI).[13]

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 during 2020-21, the Ombudsman is satisfied agencies continue to be generally compliant with the TIA Act and responsive to the Ombudsman's inspection findings.

The Ombudsman found that overall agencies demonstrated a good understanding of the requirements of the TIA Act and appropriately disclosed compliance issues to the Ombudsman.

Below is a summary of the Ombudsman's findings from the five inspections that were conducted during 2020-21. Where agencies have advised of action taken to address the Ombudsman's inspection findings, the Ombudsman will review this action during the 2021-22 inspections.

Sections 79 and 79AA: Destruction of restricted records

Sections 79 and 79AA of the TIA Act set out the requirements for agencies for destroying restricted records.[14]

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 the Department of Home Affairs (the Department), and that the relevant entry in the General Register of interception warrants has been inspected by the Minister for Home Affairs.

[13] This inspection considered ACLEI's use of telecommunications interceptions powers between 1 July and 31 December 2020. ACLEI advised it did not use the powers between 1 January and 30 June 2020 which meant the Ombudsman did not need to conduct an inspection for that period.
[14] 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 s 7(1) of the TIA Act.

At the Ombudsman's first inspection of the ACIC, the Ombudsman found the ACIC did not regularly consider when restricted records should be destroyed and had not set an internal timeframe for when destructions are considered completed 'forthwith'. The TIA Act does not create a requirement for periodic reviews of restricted records for destruction. However, to actively demonstrate compliance and noting the high level of privacy intrusion associated with intercepted data, it is the Ombudsman's view that agencies should have a process to consider whether restricted records are likely to be required for a permitted purpose and, if not, destroy the records in line with subsection 79(1) of the TIA Act. The Ombudsman suggested the ACIC establish a process to periodically identify whether restricted records should be destroyed if they are no longer likely required for a permitted purpose under subsection 79(1) of the TIA Act.

At the Ombudsman's second inspection, the ACIC advised it intends to undertake a destructions project which will result in standard procedures and timeframes for the ongoing management of restricted record destructions. The Ombudsman will revisit the ACIC's progress at their next inspection.

The Ombudsman did not make any destruction related findings under section 79 of the TIA Act for the AFP and ACLEI during 2020-21.

Section 79AA of the TIA Act requires the chief officer to cause destruction of restricted records obtained under a control order warrant in certain circumstances. The Ombudsman did not make any findings in relation to compliance with section 79AA of the TIA Act from the inspections conducted in 2020-21.

Section 80: Record keeping in connection with telecommunications interception warrants

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

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

Section 81: Record keeping in connection with telecommunications interceptions

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

The Ombudsman assessed that ACLEI was compliant with section 81 of the TIA Act. The Ombudsman made several suggestions to the AFP and the ACIC during 2020-21 regarding compliance with section 81 of the TIA Act. The Ombudsman's key suggestions are set out below.

Recording use and communication of lawfully intercepted information

Paragraph 81(1)(e) of the TIA Act requires particulars of each use by the agency of LII to be recorded as soon as practicable after the use occurs. Paragraph 81(1)(f) of the TIA Act requires particulars of each communication of LII by an officer of the agency to a

person or body that is not an officer of the agency to be recorded as soon as practicable following the communication.

Subsection 63(1) of the TIA Act prohibits a person from communicating, using or recording lawfully intercepted information (LII), subject to Part 2-6 and section 299 of the TIA Act. Under section 68 of the TIA Act, the chief officer of an agency, or an officer authorised by the chief officer, may communicate LII under certain circumstances.

At the Ombudsman's first inspection of the AFP, the Ombudsman found records and ministerial reporting were inconsistent in classifying joint task force use of LII as either internal use or external communication of LII, noting that external communication under section 68 of the TIA Act requires approval by an authorised officer. The Ombudsman suggested the AFP take steps to ensure all staff consistently record the use and communication of LII in accordance with section 81 of the TIA Act. The AFP advised it has updated templates to provide further guidance to staff.

At the Ombudsman's first inspection of the ACIC, the Ombudsman found instances where records insufficiently recorded details of use and communication of LII. At the second inspection, the ACIC advised it had updated its use and communication log template, however this template had not been released for use for the relevant records period. Despite interim measures taken to manually review logs and communicate record keeping expectations to staff, the Ombudsman found further instances where records insufficiently recorded use and communication. The Ombudsman also found the ACIC's compliance training resources did not detail expectations for recording particulars of use and communication. The Ombudsman suggested the ACIC ensure that ongoing training and compliance programs cover the specific requirements for record keeping. The ACIC advised it is in the process of reviewing its training.

Similarly, at the Ombudsman's second inspection of the AFP, the Ombudsman found several instances where records insufficiently recorded details of use and communication of LII. The Ombudsman advised where final records did adequately record use and communication, this was due to active quality assurance at the end of the administrative process. The AFP's quality assurance of records is best practice. However, its ability to provide reports to the Minister within the legislative timeframe was impacted by the need to seek further detail and clarification from investigators to address insufficiencies in the original records. The Ombudsman suggested the AFP identify and implement strategies to improve the quality of these records as they are completed in the first instance (before the quality assurance stage). The AFP advised of system improvements being undertaken to address this suggestion.

Keeping records of lawfully intercepted information given in evidence

Paragraph 81(1)(g) of the TIA Act requires an agency to record particulars of each occasion when, to the knowledge of an officer of the agency, LII was given in evidence in a relevant proceeding in relation to the agency.

At the Ombudsman's first inspection the ACIC had implemented a new process for keeping records of each occasion where LII was given in evidence. This new process included a 3-monthly review of these records as a quality control measure. The Ombudsman suggested the ACIC update its policy and procedural documents to reflect the new process and incorporate it into the ACIC's training regime, so all staff are aware

of their record-keeping obligations. At the Ombudsman's second inspection of the ACIC, the Ombudsman found no further action was taken to formalise the new process in policy and training materials. The Ombudsman also found records were incomplete. As a result, the Ombudsman reiterated the suggestion. In response, the ACIC advised of changes made to address the Ombudsman's suggestion including updates to policy and procedure.

Recording the particulars of telephone applications

Paragraph 81(1)(a) of the TIA Act requires an agency to record the particulars of each telephone application for an interception warrant made by the agency as soon as practicable after the application is made. The Ombudsman looks for contemporaneous records that set out the particulars of what information was given to the eligible Judge or nominated AAT member during the telephone application (as required under section 43 of the TIA Act) and the outcome of that application.

At the Ombudsman's first inspection the Ombudsman identified the ACIC did not have specific policies or procedures for telephone applications. The Ombudsman reviewed two telephone applications. In one instance, the Ombudsman could not locate any contemporaneous record of the particulars of the telephone application and were not satisfied the ACIC met its record keeping obligation under paragraph 81(1)(a) of the TIA Act. In the other instance, limited notes were recorded shortly after the warrant was issued. The Ombudsman suggested the ACIC establish comprehensive procedures and guidance for making telephone applications. The Ombudsman also suggested the ACIC's procedures include a mechanism to ensure it can consistently meet the record keeping requirements under paragraph 81(1)(a) of the TIA Act. The ACIC has subsequently implemented guidance on making telephone applications.

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

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

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 agencies complied with any corresponding obligations on interception under Chapter 2 of the TIA Act. The Ombudsman identified the following key issues.

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

Section 7 of the TIA Act prohibits the interception of telecommunications except in certain instances, such as under a warrant. Section 63 of the TIA Act prevents a person from dealing with LII, intercepted information obtained in contravention of section 7 of the TIA Act, or interception warrant information, unless an exemption under Part 2-6 or section 299 applies.

At each inspection of both the ACIC and the AFP, the Ombudsman found challenges in confirming the link between some internet data interceptions and the target subject to a warrant. This issue arises where the agency is unable to demonstrate whether

intercepted internet data is linked to the service authorised by the warrant, due to the format in which the information is received from the carrier.

At the Ombudsman's first inspection of the AFP, the Ombudsman found one instance where the AFP was unable to demonstrate this link and another instance where the AFP had to make subsequent enquiries to the carrier to demonstrate the link. The Ombudsman suggested the AFP continue to work with telecommunications carriers to ensure that records directly substantiate the link between intercepted internet data and the service listed on the warrant. At the Ombudsman's second inspection of the AFP, the Ombudsman was able to confirm the link between intercepted data and targets for all warrants inspected for the period with AFP technical assistance. The Ombudsman found the AFP had implemented a process to confirm the link between intercepted information and the target by analysing metadata provided with the intercepted information and suggested the AFP formalise this process in policy and procedural documentation. The AFP advised the Ombudsman it has developed a standard operating procedure to implement this.

At the Ombudsman's first inspection the ACIC disclosed six instances, and the Ombudsman found an additional instance, where initial information available to the Ombudsman did not establish a connection between the intercepted internet data and the service relevant to the warrant. Subsequently, using additional technical assistance the ACIC was able to provide sufficient information to demonstrate a link between the intercepted information and the target in all but one instance. The ACIC quarantined intercepted information in relation to the unresolved instance. The Ombudsman suggested the ACIC keep sufficient records to demonstrate the link between intercepted internet data and the service relevant to the warrant. The Ombudsman also suggested the ACIC review current data vetting processes regarding internet data intercepts to ensure it is only dealing with LII and formalise these data vetting processes to ensure they are undertaken consistently. At the Ombudsman's second inspection, the ACIC confirmed its procedure for establishing the link between intercepted internet data and the target, however policy and procedural documentation did not demonstrate steps were taken at the outset of each relevant interception to ensure this link is made. As a result of these findings, the Ombudsman made three recommendations:

- The ACIC make and keep sufficient records to ensure all intercept formats enable individual intercepted sessions to be linked to the target as specified in the warrant.
- The ACIC review current data vetting processes to ensure any intercepted information for which the link to the target is yet to be verified is quarantined until confirmation is received and placed on file.
- The ACIC formalise technical vetting and quality assurance processes in policy and procedural documentation, such as verifying the correct target value for an interception is used, to ensure these processes are undertaken consistently.

In response to the Ombudsman's recommendations, the ACIC advised it has implemented risk control measures within relevant procedures for internet protocol intercepts and additional vetting procedures and is reviewing its policy and procedures.

Unlawfully intercepted information

Section 7 of the TIA Act prohibits the interception of telecommunications except in certain instances, such as under a warrant. Section 63 of the TIA Act prevents a person from dealing with LII, intercepted information obtained in contravention of section 7 of the TIA Act, or interception warrant information, unless an exemption under Part 2-6 or section 299 applies.

At the Ombudsman's first inspection of the AFP, it was identified that several sessions of intercepted data that related to a service number not listed on the warrant. The AFP advised the Ombudsman this was due to a configuration error. The Ombudsman suggested the AFP quarantine the intercepted information and review. If advised that it has unlawfully intercepted information, the AFP should identify any use or communication of the information and seek further advice on the appropriate action. The Ombudsman also suggested the AFP track configuration errors and remedial action to facilitate ongoing improvement to its technical quality assurance procedures. In response, the AFP advised the Ombudsman that the unlawfully intercepted product had been quarantined and had not been used or communicated. The AFP also advised it had implemented changes to improve technical quality assurance procedures.

Before the Ombudsman's second inspection the AFP disclosed one instance where interception of an incorrect service number was enabled by the carrier and received by the AFP due to an administrative error in the connection request. The AFP identified the issue promptly and notified the carrier who then re-provisioned interception of the correct service number. During the inspection, the Ombudsman confirmed the AFP quarantined the unlawfully intercepted information, which had not been further distributed.

Communication of lawfully intercepted information without section 68 authorisation

Under section 68 of the TIA Act the chief officer of an agency, or an officer authorised by the chief officer, may communicate LII under certain circumstances.

At the Ombudsman's first inspection of the AFP, the AFP disclosed one instance where it communicated LII to another agency, but the communication was not made by either the chief officer or an officer authorised by the chief officer. The Ombudsman identified a similar additional instance during the inspection. In both instances, the AFP obtained retrospective approval under s 68 of the TIA Act. The Ombudsman will review at its next inspection.

Requirement to notify a carrier when a warrant is issued and revoke a warrant where grounds cease to exist

Under section 60 of the TIA Act, where a warrant is issued to the agency, the agency must inform the relevant carrier immediately and provide a certified copy of the warrant as soon as practicable.

Under subsection 57(1) of the TIA Act, the chief officer may, at any time, by signed writing, revoke a warrant issued to the agency; and must do so if satisfied the grounds on which the warrant was issued to the agency cease to exist.

At the Ombudsman's first inspection of the ACIC, the Ombudsman found one instance where a warrant was not revoked in a timely fashion after the grounds on which the warrant was issued ceased to exist. The Ombudsman suggested the ACIC remind officers of the processes regarding 'parked'[15] warrants, the importance of regularly reviewing 'parked' warrants, and the mandatory revocation requirements under section 57 of the TIA Act, where the grounds for the warrant cease to exist.

At the Ombudsman's second inspection the Ombudsman found the ACIC does not immediately notify carriers of 'parked' warrants as required by section 60 of the TIA Act. The Ombudsman suggested the ACIC seek advice on its obligation to notify carriers under section 60 of the TIA Act in relation to warrants that are, or will be 'parked' and update its policy in line with this advice. The ACIC advised it is reviewing its policy and procedures and implemented changes to its procedural documentation to provide additional guidance to staff.

Requirement to inform another agency exercising the authority of a warrant of proposed revocation

Under subsection 57(1) of the TIA Act, the chief officer may revoke a warrant issued to the agency at any time (in writing and signed). The chief officer must do so if satisfied the grounds on which the warrant was issued to the agency cease to exist. Under subsection 57(2) of the TIA Act, where another agency is exercising the authority of a warrant the chief officer must, before revoking the warrant, inform the chief officer of the other agency of the proposed revocation. The Ombudsman considers a warrant is revoked when the chief officer signs the record of their decision to revoke the warrant. The Ombudsman considers the requirement to inform another agency exercising the authority of a warrant of the proposed revocation arises prior to the chief officer signing the revocation. Subsection 57(3) of the TIA Act requires that, after revoking the warrant, the chief officer must immediately inform the chief officer of the other agency of the revocation and give a copy of the instrument of revocation to the Secretary of the Department as soon as practicable.

In one instance, ACLEI revoked a telecommunications service warrant under subsection 57(1) of the TIA Act where the authority of the warrant was exercised by the AFP. ACLEI's letter to the AFP Commissioner advising of the intention to revoke the warrant was sent after the warrant was revoked. The Ombudsman suggested ACLEI ensure it notifies other agencies exercising the authority of a telecommunications interception warrant of any proposed revocation before revoking the warrant. ACLEI undertook to implement this suggestion.

Preceding warrants left to expire when a renewal warrant takes effect

Under section 42 of the TIA Act, a written application for a telecommunications interception warrant must be accompanied by a compliant affidavit. Among other requirements the affidavit must set out the use made by the agency of information obtained by interceptions under previously issued warrants. Under paragraph 46(1)(d) of the TIA Act, in deciding to issue a telecommunications service warrant the issuing authority must be satisfied that information likely to be obtained would likely assist in

[15] An internal practice where warrants remain in force without any services or devices being actively intercepted in compelling operational circumstances exist, provided the grounds for the warrant continue to exist.

connection with the investigation by the agency of one or more serious offences. Similarly under paragraph 46A(1)(d) of the TIA Act, in deciding to issue a named person warrant the issuing authority must be satisfied that information likely to be obtained by intercepting would likely assist in connection with the investigation by the agency of one or more serious offences in which the person is involved.

Under paragraph 57(1)(b) of the TIA Act, the chief officer of an agency must revoke a warrant if satisfied the grounds on which the warrant was issued to the agency have ceased to exist. Under paragraph 57(3)(b) of the TIA Act, after revoking the warrant the chief officer must give a copy of the instrument of revocation to the Secretary of the Department as soon as practicable. Section 59 of the TIA Act provides that a warrant does not cease to be in force until the instrument of revocation is received by or on behalf of the Secretary of the Department or the warrant expires, whichever happens sooner.

At the Ombudsman's second inspection of the ACIC, the Ombudsman found one instance where a renewal warrant was issued two weeks prior to the expiry of the preceding warrant. The Ombudsman advised that it appeared the grounds for the original warrant ceased to exist at the time the renewal warrant took effect. The Ombudsman suggested the ACIC seek broader advice on the interoperation of sections 42, 46 or 46A, and 57 of the TIA Act in circumstances where a renewal warrant comes into force and a preceding warrant is not revoked.

Other administrative issues

As part of the Ombudsman's inspection methodology, the Ombudsman also reports on administrative issues, including instances where the consequences may be negligible. At the Ombudsman's inspections the Ombudsman identified, and agencies disclosed, several administrative issues:

- The Ombudsman identified instances at the AFP where affidavits did not set out all previous applications and warrants issued in relation to services and persons, as required by subsection 42(4) of the TIA Act.
- The Ombudsman identified instances where the AFP accessed stored communications under interception warrants without the intention to do so expressed in respective affidavits.
- The Ombudsman identified instances at the AFP where a copy of a revocation instrument was certified by the same officer who had signed the original instrument.
- The Ombudsman found instances at the ACIC and ACLEI where certified copies of revocation instruments were not provided to carriers as soon as practicable, as required by paragraph 60(3)(d) of the TIA Act.
- The Ombudsman advised instances were disclosed and found at the ACIC where the Secretary of the Department was not notified as soon as practicable after a warrant was issued, as required under section 59A of the TIA Act.
- The Ombudsman identified instances at the AFP and ACLEI where sections 94/94B reports to the Minister were not provided within the 3-month statutory timeframe.
- The Ombudsman identified minor inconsistencies in the ACIC and AFP's sections 94/94B reports to the Minister.
- For each agency, the Ombudsman found instances of non-compliance with prescribed forms.

Figure 1: Commonwealth Ombudsman's Telecommunications Interception Inspection Criteria

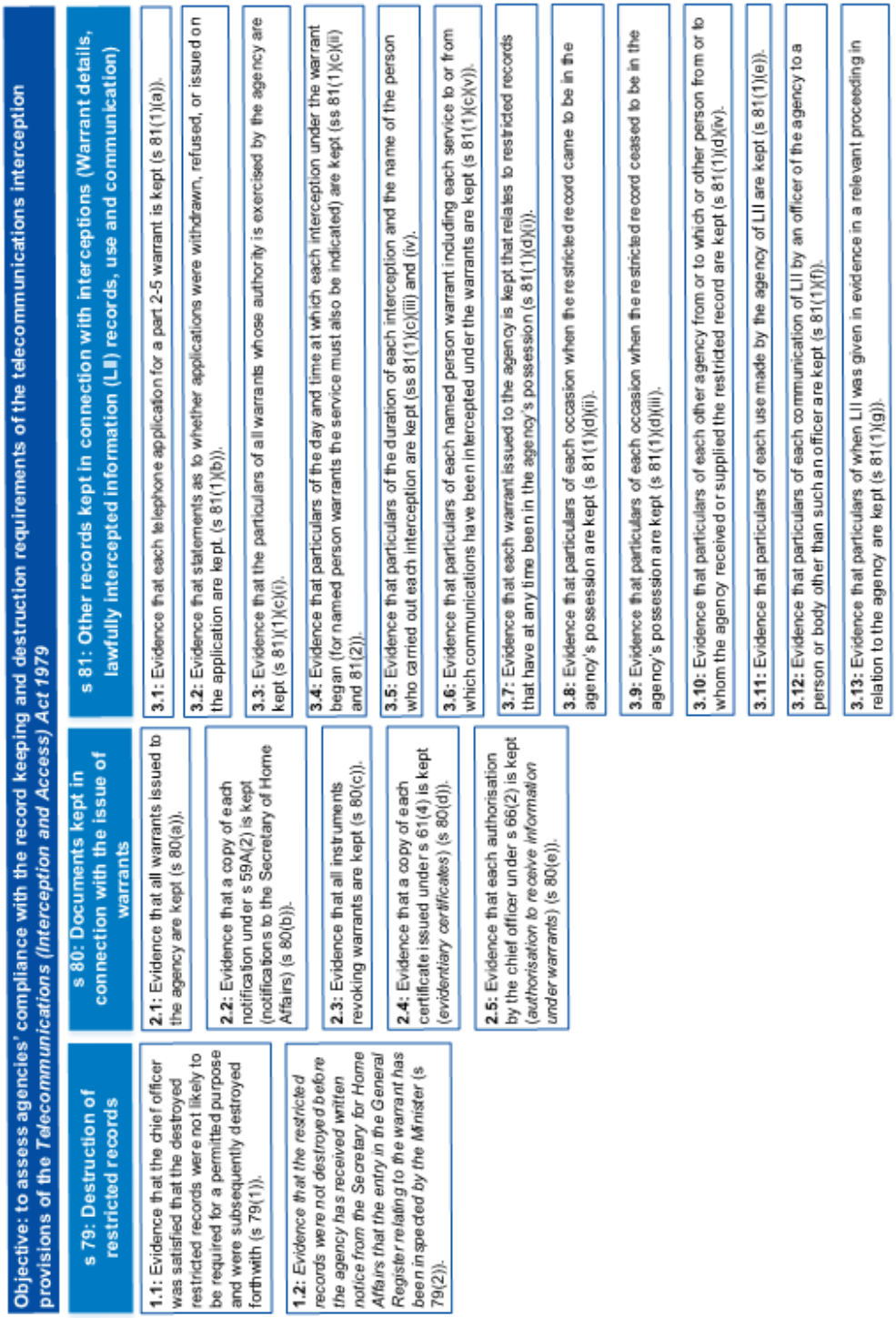
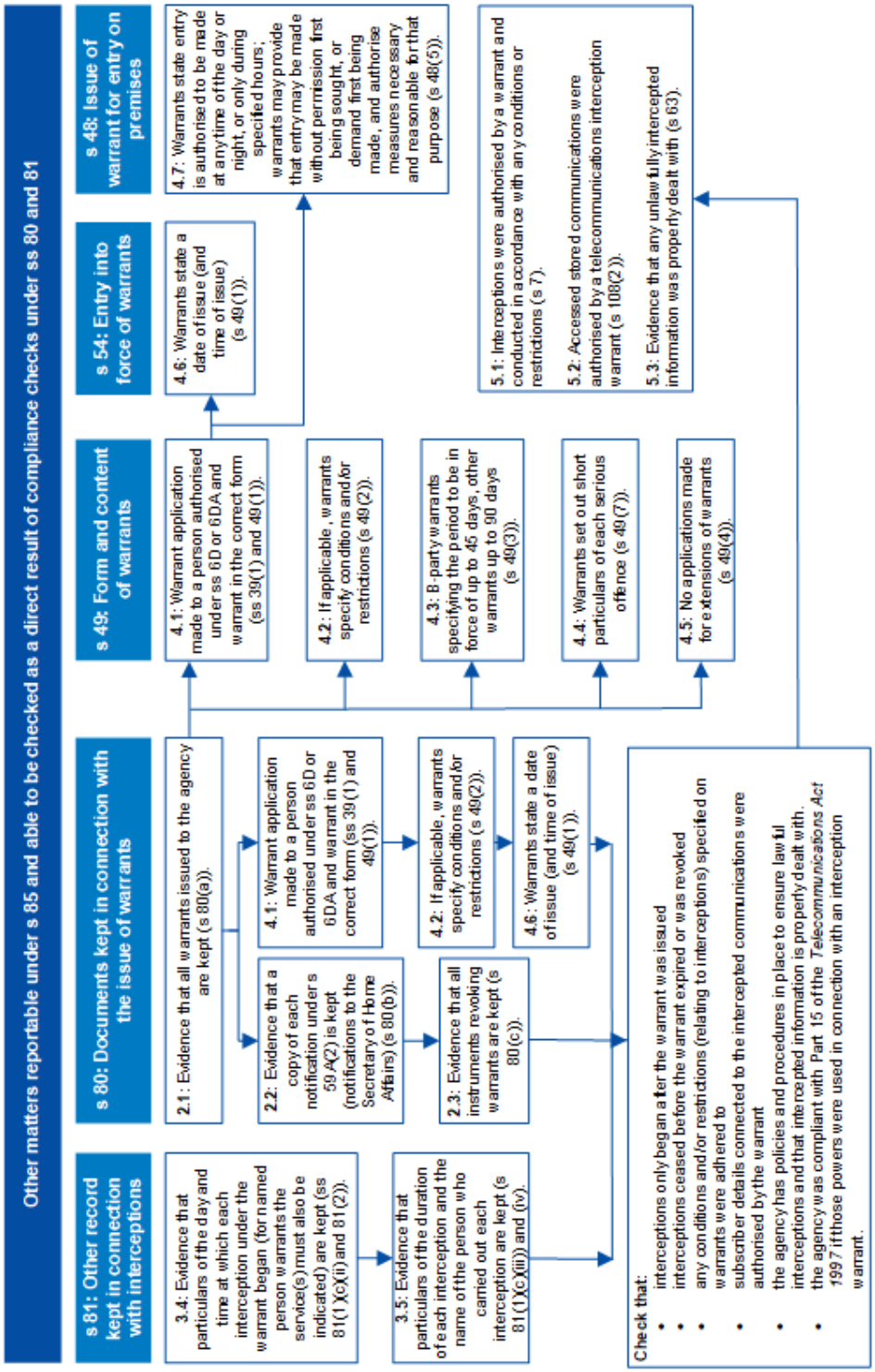


Figure 2: Other Matters reportable under section 85



CHAPTER 3 – STORED COMMUNICATIONS

Applications for stored communications warrants

Access to stored communications is regulated by Chapter 3 of the TIA Act. Chapter 3 of the TIA Act protects the privacy of people who use the Australian telecommunications network by making it an offence to access stored communications subject to limited exceptions. Authorities and bodies that are 'criminal law-enforcement agencies' under the TIA Act can apply to an issuing authority[16] for a stored communications warrant to investigate a 'serious contravention'[17] as defined in the TIA Act.

Definition

'Criminal law-enforcement agencies' are set out in section 110A of the TIA Act. These agencies include all interception agencies as well as Home Affairs, ASIC, and the ACCC. Only criminal law-enforcement agencies are eligible to apply under Chapter 3 of the TIA Act for a stored communications warrant

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

Definition

A **'serious contravention'** includes:

- serious offences (offences for which a telecommunications interception warrant can be obtained)
- offences punishable by imprisonment for a period of at least three years
- offences punishable by a fine of at least 180 penalty units ($39,960 during the reporting period) for individuals or 900 penalty units ($199,800 during the reporting period) for non-individuals such as corporations.

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

In 2020–21, 998 stored communications warrants were issued, representing a decrease of 396 from the 1,394 stored communications warrants issued in the 2019–20 period.

[16] 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.
[17] The latest penalty unit figures can be found at: www.asic.gov.au/about-asic/asic-investigations-and-enforcement/fines-and-penalties/

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

Agency	Relevant statistics	Applications for stored communications warrants		Telephone applications for stored communications warrants		Renewal applications for stored communications warrants	
		19/20	20/21	19/20	20/21	19/20	20/21
ACCC	Made	12	-	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	12	-	-	-	-	-
ACIC	Made	2	1	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	2	1	-	-	-	-
ACLEI	Made	2	-	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	2	-	-	-	-	-
AFP	Made	67	83	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	67	83	-	-	-	-
CCC (WA)	Made	1	-	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	1	-	-	-	-	-
Home Affairs	Made	2	1	-	-	-	-
	Withdrawn	-	-	-	-	-	-
	Issued	2	1	-	-	-	-
IBAC	Made	1	-	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	1	-	-	-	-	-
ICAC (NSW)	Made	2	-	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	2	-	-	-	-	-
ICAC (SA)	Made	-	2	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	-	2	-	-	-	-
LECC	Made	5	9	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	5	9	-	-	-	-
NSW CC	Made	3	-	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	3	-	-	-	-	-
NSW Police	Made	830	489	1	6	-	-
	Refused	-	-	-	-	-	-
	Issued	830	489	1	6	-	-

Agency	Relevant statistics	Applications for stored communications warrants		Telephone applications for stored communications warrants		Renewal applications for stored communications warrants	
		19/20	20/21	19/20	20/21	19/20	20/21
NT Police	Made	2	1	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	2	1	-	-	-	-
QLD CCC	Made	6	1	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	6	1	-	-	-	-
QLD Police	Made	173	129	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	173	129	-	-	-	-
SA Police	Made	34	47	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	34	47	-	-	-	-
TAS Police[18]	Made	36	40	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	36	40	-	-	-	-
VIC Police	Made	112	108	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	112	108	-	-	-	-
WA Police[19]	Made	104	87	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	104	87	-	-	-	-
TOTAL	**Made**	**1,394**	**998**	**1**	**6**	**0**	**0**
	Refused / Withdrawn	**0**	**0**	**0**	**0**	**0**	**0**
	Issued	**1,394**	**998**	**1**	**6**	**0**	**0**

[18] Correction for 2019-20: TAS Police figures relating to applications for and issuance of stored communications warrants have both been amended due to a reporting error in the 2019-20 Annual Report. As such, the total figures have also been amended. Appendix D provides both the original figures reported for the 2019-20 period, and the amended figures identified and amended by TAS Police.

[19] Correction for 2019-20: WA Police figures relating to applications for and issuance of stored communications warrants have both been amended due to a reporting error in the 2019-20 Annual Report. As such, the total figures have also been amended. Appendix D provides both the original figures reported for the 2019-20 period, and the amended figures identified and amended by WA Police.

Conditions or restrictions on stored communications warrants

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

Table 25 presents this information. In 2020–21, 532 stored communications warrants were subject to conditions or restrictions, representing a decrease of 338 compared to the 2019–20 period.

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

Agency	19/20	20/21
ACCC	3	-
AFP	-	1
NSW Police	830	489
QLD CCC	1	-
SA Police	32	41
TAS Police[20]	4	1
TOTAL	**870**	**532**

Effectiveness of stored communications warrants

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

Table 26 presents this information. In 2020–21, criminal law-enforcement agencies made 470 arrests, conducted 740 proceedings and obtained 376 convictions involving evidence obtained under stored communications warrants.

[20] Correction for 2019-20: TAS Police figures relating to stored communications warrants subject to conditions or restrictions have been amended due to a reporting error in the 2019-20 Annual Report. As such, the total figures have also been amended. Appendix D provides both the original figures reported for the 2019-20 period, and the amended figures identified and amended by TAS Police.

Table 26: Number of arrests, proceedings, and convictions made on the basis of lawfully accessed information – paragraphs 163(a)-(b)

Agency	Arrests		Proceedings		Convictions	
	19/20	20/21	19/20	20/21	19/20	20/21
ACIC	-	1	1	-	1	-
AFP	11	12	2	14	5	2
NSW CC	1	-	-	-	-	-
NSW Police	313	288	539	692	246	249
NT Police	1	-	-	-	-	-
QLD Police	139	91	7	7	7	7
SA Police	2	8	2	-	2	6
TAS Police[21]	18	5	-	10	-	10
VIC Police	60	65	17	17	37	102
TOTAL	**545**	**470**	**568**	**740**	**298**	**376**

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

Preservation notices

Under Part 3-1A of the TIA Act, criminal law-enforcement agencies can give a preservation notice to a carrier. A preservation notice allows criminal law-enforcement agencies to require a carrier to preserve stored communications that a carrier holds. The carrier is required to keep the stored communications while the notice is in force. The TIA Act provides for three types of preservation notices:

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

[21] Correction for 2019-20: TAS Police figures relating to the number of arrests made in relation to stored communications warrants have been amended due to a reporting error in the 2019-20 Annual Report. As such, the total figures have also been amended. Appendix D provides both the original figures reported for the 2019-20 period, and the amended figures identified and amended by TAS Police.

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

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

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.

Table 27 presents this information. In 2020–21, 2,092 domestic preservation notices were given, a decrease of 404 on the 2,496 given in 2019–20.

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

Agency	Domestic preservation notices issued		Domestic preservation revocation notices issued	
	19/20	20/21	19/20	20/21
ACCC	27	6	7	8
ACIC	8	4	-	1
ACLEI	2	3	-	-
AFP	500	474	263	151
CCC (WA)	3	-	2	-
Home Affairs	16	2	13	2
IBAC	6	2	-	-
ICAC (NSW)	2	1	-	-
ICAC (SA)	1	14	1	7
LECC	9	17	1	5
NSW CC	4	4	1	1
NSW Police	977	598	145	95
NT Police	31	57	25	45
QLD CCC	38	62	11	47
QLD Police	343	334	90	116
SA Police	120	127	84	77
TAS Police	95	76	49	35
VIC Police	132	159	22	23
WA Police	182	152	97	78
TOTAL	**2,496**	**2,092**	**811**	**691**

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 2020–21, the AFP reported that one foreign preservation notice was given, with no revocations.

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

Agency	Foreign preservation notices given		Foreign preservation revocation notices given	
	19/20	20/21	19/20	20/21
AFP	2	1	4	-

International assistance

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

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

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

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

Definition

An **'international offence'** is:

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

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

Table 29 presents this information. In 2020–21, the AFP was the only agency to make applications for a stored communications warrant as a result of an international assistance application, totalling five applications.

Table 29: Applications for stored communications warrants as a result of international assistance applications – paragraphs 162(1)(c) and 162(2)(ba)

Agency	Relevant statistics	Applications for stored communications warrants	
		19/20	20/21
AFP	Made	12	5
	Refused	-	-
	Issued	12	5

Paragraphs 162(1)(d) and 162(2)(e) provide that this report must list, for each international offence in respect of which a stored communications warrant application was made as a result of an international assistance application made by the agency during the year – the offence under a law of the Commonwealth, or of a State or Territory that is of the same nature as, or substantially similar to, the international offence.

The AFP applied for, and was issued five stored communications warrants[22] on behalf of other countries in relation to international offences of the following nature:

- Money laundering – Part 10.2 of the *Criminal Code*
- Conspiracy – section 11.5 of the *Criminal Code*
- Obtaining a financial advantage by deception – section 134.2 of the *Criminal Code*
- Dishonestly cause a loss to the Commonwealth – subsection 135.4(3) of the *Criminal Code*
- Serious computer offences – sections 477.1, 477.2 and 477.3 of the *Criminal Code*
- Using a telecommunications network to commit a serious offence – section 474.14 of the *Criminal Code*

Section 163A of the TIA Act provides that this report must detail information regarding the number of occasions in which lawfully accessed information or stored communications warrant information was provided to:

- a foreign country in connection with an authorisation under subsection 13A(1) of the *Mutual Assistance in Criminal Matters Act 1987*;
- the International Criminal Court in connection with an authorisation under subsection 69A(1) of the *International Criminal Court Act 2002*; and
- a War Crimes Tribunal in connection with an authorisation under subsection 25A(1) of the *International War Crimes Tribunals Act 1995.*

In 2020–21, 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 2019-20.

Ombudsman inspection report

The Commonwealth Ombudsman inspects the preservation notices and stored communications access records of all criminal law-enforcement agencies. Due to changes made in 2015, this annual report no longer includes information on inspections concerning stored communications and preservation notices. Under section 186J of the TIA Act, the Commonwealth Ombudsman continues to have a statutory obligation to report on the results of these inspections to the Minister for Home Affairs.

[22] Stored communications warrants issued on behalf of other countries can relate to more than one offence.

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

The Ombudsman's inspection reports on agency compliance with Chapters 3 and 4 of the TIA Act can be found at <www.ombudsman.gov.au>.

CHAPTER 4 – TELECOMMUNICATIONS DATA

Definition

'Telecommunications data' is information about a communication (such as the phone numbers of the people who called each other, how long they talked to each other, the email address from which a message was sent and the time the message was sent) or customer information about a service, such as customer name, address or billing details.

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

Definition

In 2020–21 the category of **'enforcement agency'** was restricted to the 20 agencies that also fall under the definition of 'criminal law-enforcement agency'. All criminal law-enforcement agencies are set out in section 110A of the TIA Act. These agencies include all interception agencies as well as Home Affairs, ASIC, and the ACCC.

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

Enforcement agencies can access existing data and criminal law-enforcement agencies can also access prospective data. Disclosure of telecommunications data must be authorised by a senior officer of the relevant enforcement agency.

Definition

'Existing data', also known as 'historical data', is information that is already in existence when an authorisation for disclosure is received by a telecommunications carrier.

'Prospective data' is telecommunications data that comes into existence during a period of time in which an authorisation is in force.

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

Existing data – enforcement of the criminal law

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

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

Table 30 provides this information. In 2020–21, 312,440 authorisations were made by agencies under section 178, an increase of 5,422 from the 307,018 authorisations made in 2019–20.

Table 30: 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	
	19/20	20/21
ACCC	123	93
ACIC	5,249	3,957
ACLEI	263	175
AFP	18,534	18,442
ASIC	1,432	536
CCC (WA)	207	174
Home Affairs[23]	3,217	5,565
IBAC	473	307
ICAC (NSW)	175	149
ICAC (SA)	196	175
LECC	829	766
NSW CC	4,734	3,538
NSW Police	116,968	103,051
NT Police	1,834	1,991
QLD CCC[24]	730	788
QLD Police	25,221	25,645
SA Police	6,229	5,656
TAS Police	5,566	5,845

[23] Correction for 2019-20: Home Affairs figures relating to authorisations made in relation to the enforcement of the criminal law have been amended due to a reporting error in the 2019-20 Annual Report. As such, the total figures have also been amended. Appendix D provides both the original figures reported for the 2019-20 period, and the amended figures identified and amended by Home Affairs.
[24] Correction for 2019-20: QLD CCC figures relating to authorisations made in relation to the enforcement of the criminal law have been amended due to a reporting error in the 2019-20 Annual Report. As such, the total figures have also been amended. Appendix D provides both the original figures reported for the 2019-20 period, and the amended figures identified and amended by the QLD CCC.

Agency	Authorisations	
	19/20	20/21
VIC Police	88,526	109,381
WA Police	26,512	26,206
TOTAL	**307,018**	**312,440**

Existing data – assist in locating a missing person

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

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

Table 31 presents this information. In 2020–21, 3,490 authorisations were made by agencies under section 178A, an increase of 462 from the 3,028 authorisations made in 2020–21.

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

Agency	Authorisations	
	19/20	20/21
AFP	159	57
NSW Police	1,684	2,121
NT Police	15	21
QLD Police	234	256
SA Police	63	83
TAS Police	78	13
VIC Police	561	728
WA Police	234	211
TOTAL	**3,028**	**3,490**

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

Section 179 of the TIA Act provides that an authorised officer of an enforcement agency can authorise the disclosure of telecommunications data if he or she is satisfied it is reasonably necessary for the enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue.

Paragraph 186(1)(b) of the TIA Act provides that this report must set out the number of authorisations made under section 179 by agencies during the year.

Table 32 presents this information. In 2020–21, 1,473 authorisations were made by agencies under section 179, an increase of 184 from the 1,289 authorisations made in 2019–20.

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

Agency	Authorisations	
	19/20	20/21
ACCC	1	24
AFP	22	23
ASIC	42	86
Home Affairs	65	18
NSW Police	1,137	1,256
NT Police	6	45
QLD CCC	1	-
QLD Police	-	7
TAS Police	10	8
WA Police	5	6
TOTAL	**1,289**	**1,473**

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 it is reasonably necessary for the investigation of a serious offence or an offence against a law of the Commonwealth, a State or a Territory that is punishable by imprisonment for at least three years. Prospective data authorisations may also authorise the disclosure of historical data.

Paragraph 186(1)(c) of the TIA Act provides that this report must set out the number of authorisations made under section 180 by agencies during the year. This information is presented in Table 33.

Table 33 also includes the average number of days prospective data authorisations were specified to be in force and the average actual number of days they remained in force during the reporting period. The average actual period in force does not include authorisations that remained in force at the end of the reporting period.

In 2020–21, 39,289 prospective authorisations were made by agencies under section 180, an increase of 6,355 on the 32,934 authorisations made in 2019–20.

Table 33: Prospective data authorisations: total made and average duration specified and actual time in force – paragraph 186(1)(c)

Agency	Number of authorisations made		Average period specified		Average period actual	
	19/20	20/21	19/20	20/21	19/20	20/21
ACIC	1,086	1,116	37	40	28	32
ACLEI	34	40	45	40	43	27
AFP[25]	4,889	6,591	42	41	29	32
ASIC	25	124	3	4	3	4
CCC (WA)	94	85	45	44	35	35
Home Affairs[26]	298	416	2	3	2	2
IBAC	267	244	43	45	38	41
ICAC (NSW)	31	19	44	45	45	35
ICAC (SA)	21	52	44	44	37	37
LECC	90	130	44	45	42	41
NSW CC	1,712	1,594	42	42	41	41
NSW Police	1,360	1,479	25	25	19	19
NT Police	248	340	41	37	34	35
QLD CCC[27]	174	244	42	43	38	42
QLD Police	4,199	4348	43	43	33	33
SA Police	468	471	29	34	20	26
TAS Police	115	114	45	45	33	29
VIC Police	14,801	17,911	13	44	12	44
WA Police	3,022	3,971	39	42	39	26
TOTAL	**32,934**	**39,289**	**35**	**42**	**30**	**37**

[25] Correction for 2019-20: AFP figures relating to prospective data authorisations have been amended due to a reporting error in the 2019-20 Annual Report. As such, the total figures have also been amended. Appendix D provides both the original figures reported for the 2019-20 period, and the amended figures identified and amended by the AFP.
[26] Correction for 2019-20: Home Affairs figures relating to prospective data authorisations have been amended due to a reporting error in the 2019-20 Annual Report. As such, the total figures have also been amended. Appendix D provides both the original figures reported for the 2019-20 period, and the amended figures identified and amended by Home Affairs.
[27] Correction for 2019-20: QLD CCC figures relating to prospective data authorisations and the average specified and actual time in force of prospective data authorisations have been amended due to a reporting error in the 2019-20 Annual Report. As such, the total figures have also been amended. Appendix D provides both the original figures reported for the 2019-20 period, and the amended figures identified and amended by the QLD CCC.

Data authorisations for foreign law enforcement

The AFP may make authorisations to obtain telecommunications data for the purposes of disclosing that data to a foreign country, the International Criminal Court or War Crimes Tribunal in connection with an investigation or proceeding within their jurisdictions, or authorise the disclosure of telecommunications data the AFP has previously obtained.

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

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

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 during the year.

In 2020–21, the AFP made the following authorisations under sections 180A, 180B, 180C, 180D of the TIA Act:

- **48 authorisations under subsection 180A(2)**
- **15 authorisations under subsection 180A(4)**
- **0 authorisations under section 180B**
- **3 authorisations under section 180C**
- **0 authorisations under section 180D**

Offences for which authorisations were made

Paragraph 186(1)(e) of the TIA Act provides that this report must set out the offences and other matters for which authorised officers of each agency made authorisations under sections 178, 178A, 179 and 180. Information relating to sections 178, 179 and 180 are presented in Tables 34, 35 and 36 respectively.

Under section 178A, 3,684 requests were made in relation to missing persons.

The offence categories listed in each table are based on the Australian and New Zealand Standard Offence Classification, published by the Australian Bureau of Statistics. In collaboration with criminal law-enforcement agencies that provided data to the department, the Department has added additional categories to better reflect the offence categories for which data authorisations may be made.

Table 34: Offences for which authorisations were made under section 178 to access existing data to enforce the criminal law – paragraph 186(1)(e)[28]

Categories of offences	ACCC	ACIC	ACLEI	AFP	ASIC	CCC (WA)	Home Affairs	IBAC	ICAC (NSW)	ICAC (SA)	LECC	NSW CC	NSW Police	NT Police	QLD CCC	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Abduction	-	-	-	161	1	-	-	-	-	-	-	33	9,522	158	-	2,239	281	665	6,253	2,967	**22,280**
Acts – injury	-	-	-	56	-	-	-	15	-	-	4	-	5,318	38	-	16	325	75	3,505	1,240	**10,592**
Bribery or corruption	-	-	175	110	-	139	73	291	12	124	644	-	0	14	276	-	44	-	1	131	**2,034**
Cartel offences	89	-	-	-	-	-	-	-	-	-	-	-	9	-	-	-	1	-	-	-	**99**
Conspire	-	-	-	114	2	-	1	-	-	-	-	-	319	9	-	3	31	-	9,089	51	**9,619**
Cybercrime	-	-	8	738	3	-	-	-	-	-	-	-	2,657	30	5	984	-	108	1,071	383	**5,987**
Dangerous acts	-	-	-	31	-	-	-	-	-	-	-	-	978	54	-	1,508	313	37	2,109	536	**5,566**
Fraud	-	-	4	1,462	521	7	367	1	135	43	5	261	12,672	88	12	654	512	332	10,331	1,557	**28,964**
Homicide	-	-	-	468	-	-	-	-	-	-	-	405	13,907	226	-	1,811	745	407	7,050	2,366	**27,385**
Illicit drug offences	-	30	7	8,883	-	-	1,796	-	-	-	85	2,421	23,930	886	238	4,251	1,762	2,291	14,879	7,052	**68,511**
Loss of life	-	-	-	14	-	-	-	-	-	-	-	4	412	9	-	564	42	-	432	103	**1,580**
Miscellaneous	-	1	-	184	59	9	1,737	-	-	-	23	76	4,415	75	257	6,345	37	115	793	371	**14,497**
Justice procedures	4	-	-	410	1	11	-	-	2	2	3	-	803	20	-	-	57	200	9,004	517	**11,034**
Organised offences	-	1	-	290	-	8	-	-	-	-	-	-	1,456	10	-	19	20	-	4	982	**2,790**
Pecuniary penalty	-	-	-	36	-	-	-	-	-	-	-	-	1,069	5	-	-	-	-	-	-	**1,110**
Public revenue	-	-	-	19	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	76	**95**

[28] Appendix E contains a description of each of the categories of offences.

Categories of offences	ACCC	ACIC	ACLEI	AFP	ASIC	CCC (WA)	Home Affairs	IBAC	ICAC (NSW)	ICAC (SA)	LECC	NSW CC	NSW Police	NT Police	QLD CCC	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
People smuggling	-	-	15	189	-	-	-	-	-	-	-	-	12	-	-	-	-	-	-	-	**216**
Weapons	-	-	-	114	-	-	88	-	-	-	-	102	1,477	6	-	40	105	71	3,340	38	**5,381**
Property damage	-	-	-	26	-	-	-	-	-	-	-	-	1,082	16	-	108	135	2	2,365	71	**3,805**
Public order offences	-	-	-	1	-	-	-	-	-	-	-	-	53	-	-	20	13	4	417	61	**569**
Robbery	-	-	-	86	-	-	-	-	-	-	-	-	7,565	100	-	1,211	222	206	6,582	1,840	**17,812**
Serious damage	-	-	-	4	-	-	-	-	-	-	-	-	357	19	-	729	99	138	3	169	**1,518**
Sexual assault	-	-	-	3,166	-	-	-	-	-	-	-	-	7,274	172	-	2,272	416	142	5,865	1,226	**20,533**
Special ACC Investigation	-	3,910	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**3,910**
Terrorism offences	-	15	-	874	-	-	6	-	-	-	-	236	196	-	-	-	6	-	413	262	**2,008**
Theft	-	-	-	869	5	-	79	-	-	6	2	-	4,763	28	-	1,073	152	660	6,756	1,441	**15,834**
Traffic	-	-	-	9	-	-	-	-	-	-	-	-	665	4	-	149	8	15	562	246	**1,658**
Unlawful entry	-	-	-	128	-	-	-	-	-	-	-	-	1,942	28	-	1,423	330	377	18,557	2,520	**25,305**
TOTAL	**93**	**3,957**	**209**	**18,442**	**592**	**174**	**4,147**	**307**	**149**	**175**	**766**	**3,538**	**102,853**	**1,995**	**788**	**25,419**	**5,656**	**5,845**	**109,381**	**26,206**	**310,692**

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	ACCC	AFP	ASIC	Home Affairs	NSW Police	NT Police	QLD Police	TAS Police	WA Police	TOTAL
Abduction	-	-	2	-	126	-	-	-	-	**128**
Acts – injury	-	-	-	-	14	-	-	-	-	**14**
Cartel offences	15	-	-	-	-	-	-	-	-	**15**
Conspire	-	-	1	-	-	-	-	-	-	**1**
Cybercrime	-	6	3	-	18	-	-	-	4	**31**
Dangerous acts	-	-	-	-	29	-	-	1	-	**30**
Fraud	-	1	69	-	82	-	-	-	-	**152**
Homicide	-	-	-	-	173	-	-	-	-	**173**
Illicit drug offences	-	-	-	-	84	-	-	-	-	**84**
Loss of life	-	-	-	-	8	-	-	-	-	**8**
Miscellaneous	-	-	39	-	45	3	-	-	-	**87**
Justice procedures	-	-	1	-	9	24	-	-	-	**34**
Organised offences	-	-	-	-	102	-	-	-	-	**102**
Pecuniary penalty	9	8	3	5	212	17	-	6	2	**262**
Public revenue	-	7	-	-	-	-	7	-	-	**14**
Weapons	-	-	-	-	1	-	-	-	-	**1**
Property damage	-	-	-	-	13	-	-	-	-	**13**

Categories of offences	ACCC	AFP	ASIC	Home Affairs	NSW Police	NT Police	QLD Police	TAS Police	WA Police	TOTAL
Public order offences	-	-	-	-	7	-	-	1	-	**8**
Robbery	-	-	-	-	213	-	-	-	-	**213**
Sexual assault	-	1	-	-	49	-	-	-	-	**50**
Terrorism offences	-	-	-	-	2	-	-	-	-	**2**
Theft	-	-	-	4	16	-	-	-	-	**20**
Traffic	-	-	-	-	49	1	-	-	-	**50**
Unlawful entry	-	-	-	-	3	-	-	-	-	**3**
TOTAL	**24**	**23**	**118**	**9**	**1,255**	**45**	**7**	**8**	**6**	**1,495**

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	ACIC	ACLEI	AFP	ASIC	CCC (WA)	Home Affairs	IBAC	ICAC (NSW)	ICAC (SA)	LECC	NSW CC	NSW Police	NT Police	QLD CCC	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Abduction	-	-	16	-	-	-	-	-	-	-	5	119	12	-	303	1	6	824	134	**1,420**
Acts – injury	-	-	11	-	-	-	-	-	-	-	-	195	2	-	16	4	1	1,064	167	**1,460**
Bribery or corruption	-	40	14	-	84	-	244	1	51	98	-	-	-	128	5	-	-	26	1	**692**
Conspire	-	-	29	-	-	-	-	-	-	-	-	7	3	-	-	1	-	1,210	13	**1,263**
Cybercrime	-	-	330	-	-	-	-	-	-	-	-	7	13	1	23	-	1	32	4	**411**
Dangerous acts	-	-	9	-	-	-	-	-	-	-	-	8	7	-	23	-	2	513	68	**630**
Fraud	-	-	449	124	-	46	-	18	1	-	119	63	1	5	133	-	1	833	286	**2,079**
Homicide	-	-	159	-	-	-	-		-	-	106	62	6	-	424	1	8	709	92	**1,567**
Illicit drug offences	17	22	4,159	-	-	85	-	-	-	23	1,221	561	257	66	2,458	2	68	3,918	1,870	**14,727**
Loss of life	-	-	4	-	-	-	-	-	-	-	5	27	1	-	-	1	-	4	-	**42**
Miscellaneous	-	-	53	6	-	229	-	-	-	8	24	71	1	44	87	-	-	52	54	**629**
Justice procedures	-	-	124	-	-	-	-	-	-	1	-	10	3	-	-	-	-	1,209	-	**1,347**
Organised offences	6	-	620	-	1	-	-	-	-	-	-	34	8	-	7	-	-	1	-	**677**
Pecuniary penalty	-	-	19	-	-	-	-	-	-	-	-	-	1	-	-	-	2	-	-	**22**
Public revenue	-	-	7	-	-	-	-	-	-	-	-	2	-	-	-	-	-	-	-	**9**

Categories of offences	ACIC	ACLEI	AFP	ASIC	CCC (WA)	Home Affairs	IBAC	ICAC (NSW)	ICAC (SA)	LECC	NSW CC	NSW Police	NT Police	QLD CCC	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
People smuggling	-	-	41	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**41**
Weapons	-	-	68	-	-	23	-	-	-	-	54	77	3	-	111	-	1	870	79	**1,286**
Property damage	-	-	2	-	-	-	-	-	-	-	-	14	-	-	-	-	-	169	-	**185**
Public order offences	-	-	1	-	-	-	-	-	-	-	-	1	-	-	-	-	-	103	-	**105**
Robbery	-	-	44	-	-	-	-	-	-	-	-	78	9	-	205	-	5	1,083	247	**1,671**
Serious damage	-	-	-	-	-	-	-	-	-	-	-	5	6	-	33	-	-	26	64	**134**
Sexual assault	-	-	160	-	-	2	-	-	-	-	-	37	6	-	54	1	2	543	55	**860**
Special ACC Investigation	1,087	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**1,087**
Terrorism offences	3	-	184	-	-	-	-	-	-	-	60	1	-	-	12	-	-	69	74	**403**
Theft	-	-	285	1	-	33	-	-	-	-	-	63	-	-	155	-	8	1,318	233	**2,096**
Traffic	-	-	2	-	-	-	-	-	-	-	-	6	-	-	-	4	-	60	14	**86**
Unlawful entry	-	-	48	-	-	-	-	-	-	-	-	31	1	-	299	4	**9**	3,275	516	**4,183**
TOTAL	**1,113**	**62**	**6,838**	**131**	**85**	**418**	**244**	**19**	**52**	**130**	**1,594**	**1,479**	**340**	**244**	**4,348**	**19**	**114**	**17,911**	**3,971**	**39,112**

Age of data under disclosure

Paragraph 186(1)(f) 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.

Table 37 provides this information. The statistics are split into successive periods of three months and include the total number of authorisations made for data held for the lengths of time specified, in accordance with subsection 180(1C) of the TIA Act. The information covers the mandatory retention period for telecommunications data and provides an indication of how frequently data is accessed over two years.

In 2020–21, 269,682 authorisations were for data 0–3 months old. This includes authorisations for 'point in time' information without an identifiable age, such as current subscriber information and current information held in the Integrated Public Number Database,[29] which have been recorded as '0' months old and are included in the 0–3 month field.

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

Agency	Age of disclosure									
	0 – 3 mths	3 – 6 mths	6 – 9 mths	9 – 12 mths	12 – 15 mths	15 – 18 mths	18 – 21 mths	21 – 24 mths	Over 24 mths	TOTAL
ACCC	16	9	5	8	11	2	11	3	52	**117**
ACIC	3,262	411	98	42	75	11	19	3	36	**3,957**
ACLEI	128	14	29	8	5	4	5	-	22	**215**
AFP	11,685	2,899	877	898	523	232	186	267	955	**18,522**
ASIC	390	52	36	42	29	5	16	12	40	**622**
CCC (WA)	130	5	9	12	1	3	1	-	13	**174**
Home Affairs	1,222	550	206	180	169	20	24	29	80	**2,480**
IBAC	266	-	5	2	10	9	-	3	12	**307**
ICAC (NSW)	53	2	7	5	3	3	-	3	73	**149**
ICAC (SA)	53	34	18	19	1	1	2	-	47	**175**

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

Agency	Age of disclosure									
	0 – 3 mths	3 – 6 mths	6 – 9 mths	9 – 12 mths	12 – 15 mths	15 – 18 mths	18 – 21 mths	21 – 24 mths	Over 24 mths	TOTAL
LECC	618	47	21	19	6	2	2	-	51	**766**
NSW CC	2,805	181	120	137	81	19	64	14	117	**3,538**
NSW Police	95,306	4,060	1,838	1,816	694	564	284	325	1,541	**106,428**
NT Police	1,873	46	18	18	21	5	11	6	63	**2,061**
QLD CCC	468	111	48	35	43	19	22	7	35	**788**
QLD Police	21,046	1,472	984	625	494	282	246	165	591	**25,905**
SA Police	3,742	755	325	309	119	66	71	45	326	**5,758**
TAS Police	5,020	372	204	132	33	30	26	12	138	**5,967**
VIC Police	101,924	3,857	1,649	890	677	225	103	164	620	**110,109**
WA Police	19,675	2,406	1,187	809	533	299	196	190	911	**26,206**
TOTAL	**269,682**	**17,283**	**7,684**	**6,006**	**3,528**	**1,801**	**1,289**	**1,248**	**5,723**	**314,244**

Types of retained data

Paragraphs 186(1)(g)-(h) of the TIA Act provide that this report must set out the number of occasions during the reporting period that agencies made authorisations for retained data which included information from the data subsets identified in subsection 187AA(1). Data within item 1 of that subsection is typically considered 'subscriber data' and includes information identifying the user of a telecommunications service. Data within items 2–6 of that subsection are typically considered 'traffic data' and include information such as the time, duration, and source of a communication.[30] 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)[31]

Agency	Item 1: subscriber data	Items 2 – 6: traffic data
ACCC	65	52
ACIC	2,308	1,649
ACLEI	87	88
AFP	15,190	3,332
ASIC	366	256
CCC (WA)	110	64
Home Affairs	2,941	1,207
IBAC	221	93
ICAC (NSW)	104	45
ICAC (SA)	96	79
LECC	599	167
NSW CC	1,735	1,803
NSW Police	72,763	33,665
NT Police	1,621	465
QLD CCC	561	227
QLD Police	18,570	6,078
SA Police	3,684	2,074
TAS Police	4,955	893
VIC Police	77,743	32,366
WA Police	19,694	6,512
TOTAL	**223,413**	**91,115**

[30] Appendix F further explains the type of data included in items 1–6 of the table at subsection 187AA(1).
[31] An agency can request both types of data in a single request.

Journalist information warrants

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

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

In 2020–21, no JIW warrants were issued. In 2019–20 one JIW was issued to QLD CCC under s178 of the TIA Act.

Industry estimated cost of implementing data retention

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

Information collected from industry by the Australian Communications and Media Authority (ACMA), shows the cost of complying with the data retention obligations. This information is set out in Table 39.

Table 39 further sets out the costs recovered from criminal law-enforcement agencies for the purpose of complying with their data retention obligations.

Table 39: Industry Capital Costs 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)
2019–20	$21,246,398.52	$11,165,966.50
2020–21	$25,262,114.03	$13,385,407.50
TOTAL	**$238,274,916.41**	**$50,366,597.73**

CHAPTER 5 – INDUSTRY ASSISTANCE

Part 15 of the Telecommunications Act sets out an industry assistance framework providing a structure through which Australian agencies and the communications industry can work together to address technological obstacles to investigations into serious crime and national security threats.

Requests and notices

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

- **Technical Assistance Request (TAR):** Agencies can request voluntary help from designated communications providers[32] where they are willing and able to give assistance.
- **Technical Assistance Notice (TAN):** Agencies can compel designated communications providers to give assistance where they already have the technical capability to do so.
- **Technical Capability Notice (TCN):** Agencies can require providers build limited capabilities to help law enforcement and security authorities. The Attorney-General and the Minister for Communications must both agree to give a designated communications provider a TCN.

Table 40: Eligible agencies under Part 15 of the Telecommunications Act

Agency	Industry assistance powers available to agencies		
	TAR	TAN	TCN
Interception Agencies[33]	✓	✓	✓
ASD	✓	✗	✗
ASIO	✓	✓	✓
ASIS	✓	✗	✗

Definition

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

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

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

The industry assistance framework provides that:

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

Definition

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

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

The framework contains numerous limitations and safeguards including:

- prohibiting assistance that creates 'systemic weaknesses' in encrypted devices and communication systems. This includes a prohibition on requesting or requiring providers to refrain from fixing vulnerabilities or making their systems more secure, build a decryption capability, or reduce the broader security of their systems;
- to see the content of personal communications or intercept communications, agencies must still obtain the necessary warrant or authorisation under the relevant law of the Commonwealth, States or Territories (such as a warrant under the TIA Act); 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 chief officers of interception agencies during the year, and the number of TCNs given during the year that were directed towards ensuring designated communications providers were capable of giving help to interception agencies.

This information is presented in Table 41. In 2020–21, 25 TARs were given by interception agencies to designated communications providers. This increased by 14 from the previous year.

One TAN was given by NSW Police. This was the first TAN given to a designated communications provider since the commencement of the framework.

No TCNs were sought by interception agencies.

Table 41: Number of Technical Assistance Requests, Technical Assistance Notices, and Technical Capability Notices given between 1 July 2020 and 30 June 2021 – paragraphs 317ZS(1)(a)–(c) of the Telecommunications Act

Agency	Requests or notices given			
	Technical Assistance Request	Technical Assistance Notice	Technical Capability Notice	TOTAL
ACIC	2	-	-	**2**
AFP	2	-	-	**2**
NSW Police	16	1	-	**17**
VIC Police	5	-	-	**5**
TOTAL	**25**	**1**	**0**	**26**

Offences enforced through industry assistance

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

Table 42 provides this information for the 2020–21 period.

The offence categories listed in the table are based on the Australian and New Zealand Standard Offence Classification, published by the Australian Bureau of Statistics. The Department of Home Affairs has added additional categories to better reflect the offence categories for which requests and notices may be given.[34]

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

Table 42: Kinds of serious Australian offences enforced through Technical Assistance Requests – paragraph 317ZS(1)(d) of the Telecommunications Act

Categories of offences	ACIC	AFP	NSW Police	VIC Police	TOTAL
Acts intended to cause injury	-	-	1	-	1
Cybercrime offences	-	1	-	-	1
Homicide	-	-	5	2	7
Illicit drug offences	-	1	3	3	7
Organised offences	2	-	6	-	8
Sexual assault	-	-	1	-	1
TOTAL	**2**	**2**	**16**	**5**	**25**

Table 43: Kinds of serious Australian offences enforced through Technical Assistance Notices – paragraph 317ZS(1)(d) of the Telecommunications Act

Categories of offences	NSW Police	Total
Homicide	1	1

Oversight of industry assistance powers

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

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

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

Compulsory powers carry additional oversight measures to ensure they are used appropriately.

Where a State or Territory law enforcement agency issues a notice to compel technical assistance through a TAN, it must first be reviewed by the AFP Commissioner.

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

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

Designated communications providers may make a complaint to the relevant oversight body for the agency that issued the request or notice. In the case of ASIO, ASD and ASIS, this is the IGIS. In the case of interception agencies, this is the Commonwealth Ombudsman. Additionally, in the case of State and Northern Territory Police, providers are advised that they may contact the inspecting authority of the relevant State or the Northern Territory to complain about an assistance instrument they have been issued.[35]

[35] Further information on Part 15 of the Telecommunications Act including detailed administrative guidance can be found on the website of the Department of Home Affairs, at <www.homeaffairs.gov.au>.

CHAPTER 6 – FURTHER INFORMATION

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

National Security Policy Branch

Department of Home Affairs

PO Box 25

BELCONNEN ACT 2616

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

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

APPENDIX A – LISTS OF TABLES AND FIGURES

Table	Table title	Page #
Table 1:	Categories of serious offences specified in telecommunications interception warrants – paragraphs 100(1)(f), 100(1)(g), 100(2)(f) and 100(2)(g)	9
Table 2:	Number of Federal Court Judges, Family Court Judges, Federal Circuit Court Judges and nominated AAT members to issue telecommunications interception warrants – paragraph 103(ab)	11
Table 3:	Number of interception warrants issued by Federal Court judges, Family court judges, Federal Circuit Court judges and nominated AAT members – paragraph 103(ab)	12
Table 4:	Applications, telephone applications and renewal applications for interception warrants – paragraphs 100(1)(a)-(c) and 100(2)(a)-(c)	13
Table 5:	Interception warrants issued with specific conditions or restrictions – paragraphs 100(1)(e) and 100(2)(e)	16
Table 6:	Arrests on the basis of lawfully intercepted information – paragraphs 102(1)(a) and 100(2)(e)	17
Table 7:	Prosecutions per offence category in which lawfully intercepted information was given in evidence – paragraphs 102(1)(b)-(c) and 102(2)(b)-(c)	18
Table 8:	Convictions per offence category in which lawfully intercepted information was given in evidence – paragraphs 102(1)(b)-(c) and 102(2)(b)-(c)	19
Table 9:	Original applications for named person warrants, telephone applications for named person warrants, and renewal applications – paragraphs 100(1)(ea) and 100(2)(ea)	21
Table 10:	Named person warrants issued with specific conditions or restrictions – paragraphs 100(1)(ea) and 100(2)(ea)	23
Table 11:	Number of named person warrants by reference to services intercepted under the warrant– paragraphs 100(1)(eb) and 100(2)(eb)	23
Table 12:	Total number of services intercepted under service-based named person warrants – paragraphs 100(1)(ec) and 100(2)(ec)	24
Table 13:	Total number of services and devices intercepted under device-based named person warrants – paragraphs 100(1)(ec) and 100(2)(ec)	25
Table 14:	Applications for B-Party warrants, telephone applications for B-Party warrants, and renewal applications – paragraphs 100(1)(ed) and 100(2)(ed)	26
Table 15:	B-Party warrant issued with conditions or restrictions – paragraphs 100(1)(ed) and 100(2)(ed)	26
Table 16:	Duration of original and renewal telecommunications interception warrants – paragraphs 101(1)(a)-(d) and 101(2)(a)-(d)	27
Table 17:	Duration of original and renewal B-Party warrants – paragraphs 101(1)(da) and 102(2)(da)	28
Table 18:	Number of final renewals – paragraphs 101(1)(e) and 101(2)(e)	28
Table 19:	Percentage of eligible warrants – paragraphs 102(3) and 102(4)	29
Table 20:	Number of interceptions carried out on behalf of other agencies – paragraph 103(ac)	31
Table 21:	Total expenditure incurred by each agency in connection with the execution of telecommunications interception warrants and average expenditure per telecommunications interception warrant – paragraphs 103(a) and 103(aa).	32
Table 22:	Recurrent interception costs per agency	32
Table 23:	Emergency service facility declarations – paragraph 103(ad)	33
Table 24:	Applications, telephone applications and renewal applications for stored communications warrants – paragraphs 162(1)(a)-(b) and 162(2)(a)-(b)	46
Table 25:	Stored communications warrants subject to conditions or restrictions – paragraph 162(2)(d)	48
Table 26:	Number of arrests, proceedings, and convictions made on the basis of lawfully accessed information – paragraphs 163(a)-(b)	49
Table 27:	Domestic preservation notices – subsection 161A(1)	50
Table 28:	Foreign preservation notices – subsection 161A(2)	51
Table 29:	Applications for stored communications warrants as a result of international assistance applications – paragraph 162(1)(c)	51
Table 30:	Number of authorisations made by a criminal law-enforcement agency for access to existing information or documents in the enforcement of a criminal law – paragraph186(1)(a)	55
Table 31:	Number of authorisations made for access to existing information or documents for the location of missing persons – paragraph 186(1)(aa)	56

Table	Table title	Page #
Table 32:	Number of authorisations made by a criminal law-enforcement agency for access to existing information or documents in the enforcement of a law imposing a pecuniary penalty or protection of the public revenue – paragraph 186(1)(b)	57
Table 33:	Prospective data authorisations: total made and average duration specified and actual time in force – paragraph 186(1)(c)	58
Table 34:	Offences for which authorisations were made under section 178 to access existing data to enforce the criminal law – paragraph186(1)(e)	60
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)	62
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)	64
Table 37:	Periods for which retained data was held by carrier before authorised disclosure paragraph 186(1)(f)	66
Table 38:	Types of retained data disclosed in authorisations – paragraphs 186(1)(g) and 186(1)(h)	68
Table 39:	Industry Capital Costs of data retention – section 187P(1A)	69
Table 40:	Eligible agencies under Part 15 of the Telecommunications Act	70
Table 41:	Number of Technical Assistance Requests, Technical Assistance Notices, and Technical Capability Notices given between 1 July 2020 and 30 June 2021 – paragraphs 317ZS(1)(a)–(c) of the Telecommunications Act	72
Table 42:	Kinds of serious Australian offences enforced through Technical Assistance Requests – paragraph 317ZS(1)(d) of the Telecommunications Act	73
Table 43:	Kinds of serious Australian offences enforced through Technical Assistance Notices – paragraph 317ZS(1)(d) of the Telecommunications Act	73

Figure	Figure Title	Page #
Figure 1:	Commonwealth Ombudsman's Telecommunications Interception Inspection Criteria	43
Figure 2:	Other matters reportable by the Commonwealth Ombudsman under section 85	44

APPENDIX B – INTERCEPTION AGENCIES UNDER THE TIA ACT

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

APPENDIX C – CATEGORIES OF SERIOUS OFFENCES UNDER THE TIA ACT

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

APPENDIX D – UPDATED FIGURES FOR PREVIOUS REPORTING PERIODS

AFP 2008–20:

In 2020 the AFP discovered compliance issues dating back to 2008 regarding record keeping and reporting of requests to telecommunications carriers under section 180 of the TIA Act. The authorisations were made by ACT Policing and relate to prospective data. The AFP has provided updates to the number of authorisations made for the reporting periods identified below, but do not have the figures to be able to update other statistics, such as days in force. The corrected figures are reported below:

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

Number of authorisations made												
Agency	08/09 Original	08/09 Updated	09/10 Original	09/10 Updated	10/11 Original	10/11 Updated	11/12 Original	11/12 Updated	12/13 Original	12/13 Updated	13/14 Original	13/14 Updated
AFP	103	104[36]	148	149[37]	683	912[38]	194	314[39]	683	807[40]	1,037	1,411[41]
TOTAL	2,571	2,572	3,804	3,805	4,836	5,065	5,811	5,931	7,532	7,656	13,115	13,489

Number of authorisations made												
Agency	14/15 Original	14/15 Updated	15/16 Original	15/16 Updated	16/17 Original	16/17 Updated	17/18 Original	17/18 Updated	18/19 Original	18/19 Updated	19/20 Original	19/20 Updated
AFP	1,624	2,284[42]	2,592	2,834[43]	3,045	3,357[44]	3,700	3,916[45]	4,707	4,871[46]	4,835	4,889[47]
TOTAL	17,429	18,089	20,105	20,347	20,540	20,852	23,944	24,160	27,771	27,950[48]	32,856	32,934[49]

[36] Correction refers to Table 57, page 76, 2008-09 TIA Act Annual Report.
[37] Correction refers to Table 59, page 80, 2009-10 TIA Act Annual Report.
[38] Correction refers to Table 59, page 66, 2010-11 TIA Act Annual Report.
[39] Correction refers to Table 58, page 70, 2011-12 TIA Act Annual Report.
[40] Correction refers to Table 34, page 54, 2012-13 TIA Act Annual Report.
[41] Correction refers to Table 36, page 52, 2013-14 TIA Act Annual Report.
[42] Correction refers to Table 36, page 48, 2014-15 TIA Act Annual Report.
[43] Correction refers to Table 37, page 46, 2015-16 TIA Act Annual Report.
[44] Correction refers to Table 33, page 40, 2016-17 TIA Act Annual Report.
[45] Correction refers to Table 31, page 50, 2017-18 TIA Act Annual Report and to Appendix D, pages 86-7, 2019-20 TIA Act Annual Report.
[46] Correction refers to Table 33, page 57, 2018-19 TIA Act Annual Report and to Appendix D, page 90, 2019-20 TIA Act Annual Report.
[47] Correction refers to Table 32, page 60, 2019-20 TIA Act Annual Report.
[48] This figure includes updates from the QLD CCC which are identified in this Appendix.
[49] This figure includes updated from Home Affairs and the QLD CCC which are identified in this Appendix.

Home Affairs 2019-20:

Home Affairs identified corrections regarding access to telecommunications data for the 2019-20 reporting period. The below details both the original figures provided for the 2019-20 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 in the enforcement of a criminal law – paragraph 186(1)(a)

Agency	Authorisations	
	19/20 Original	19/20 Updated
Home Affairs[50]	3,214	3,217
TOTAL	**306,995**	**307,018**[51]

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

	Number of authorisations made	
Agency	**19/20 Original**	**19/20 Updated**
Home Affairs[52]	296	298
TOTAL[53]	**32,856**	**32,934**

Offences for which authorisations were made under section 178 to access existing data to enforce the criminal law – paragraph 186(1)(e)[54]

Categories of offences	19/20 Original	19/20 Updated
Bribery or corruption	5	11
Fraud	1,346	1,368
Illicit drug offences	1,502	1,586
Miscellaneous	54	59
Organised offences	-	7
Pecuniary penalty	-	1
People smuggling	57	59
Weapons	224	223
Theft	78	83
TOTAL (Home Affairs)	**3,266**	**3,397**

[50] Corrections refer to Table 29, page 56, 2019-20 TIA Act Annual Report.
[51] This figure includes updates from the QLD CCC which are identified in this Appendix.
[52] Corrections refer to Table 32, page 60, 2019-20 TIA Act Annual Report.
[53] These total figures include updates from the AFP and QLD CCC which are identified in this Appendix.
[54] Corrections refer to Table 34, pages 63-4, 2019-20 TIA Act Annual Report.

Offences against which authorisations were made under section 179 for access to existing data for the enforcement of a law imposing a pecuniary penalty or protection of the public revenue – paragraph 186(1)(e)[55]

Categories of offences	19/20 Original	19/20 Updated
Fraud	38	90
Illicit drug offences	19	19
Pecuniary penalty	3	3
Weapons	5	5
TOTAL (Home Affairs)	**65**	**117**

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)[56]

Categories of offences	19/20 Original	19/20 Updated
Bribery or corruption	4	4
Fraud	179	185
Illicit drug offences	55	56
People smuggling	2	2
Weapons	54	55
TOTAL (Home Affairs)	**294**	**302**

Periods which retained data was held by carrier before authorised disclosure – paragraph 186(1)(f)[57]

Home Affairs	Age of disclosure									
	0 – 3 mths	3 – 6 mths	6 – 9 mths	9 – 12 mths	12 – 15 mths	15 – 18 mths	18 – 21 mths	21 – 24 mths	Over 24 mths	TOTAL
19/20 Original	2,625	425	200	105	70	33	24	10	77	**3,569**
19/20 Updated	2,627	429	201	106	72	33	24	10	78	**3,580**

Types of retained data disclosed in authorisations – paragraphs 186(1)(g) and 186(1)(h)[58]

Home Affairs	Item 1: subscriber data	Items 2 – 6: traffic data
19/20 Original	2,618	1,266
19/20 Updated	2,617	1,282

[55] Corrections refer to Table 36, pages 67-8, 2019-20 TIA Act Annual Report.
[56] Corrections refer to Table 37, pages 69-70, 2019-20 TIA Act Annual Report.
[57] Corrections refer to Table 38, page 72, 2019-20 TIA Act Annual Report.
[58] Corrections refer to Table 39, page 73, 2019-20 TIA Act Annual Report.

LECC 2017–18:

LECC identified corrections regarding domestic preservation revocation notices issued for the 2017–18 reporting period. The below details both the original figures provided for the 2017–18 Annual Report and the amended figures as identified and corrected .

Domestic preservation notices – subsection 161A(1)[59]

Agency	Domestic preservation revocation notices issued	
	17/18 Original	17/18 Updated
LECC	7	6
TOTAL	495	494

QLD CCC 2018–19 and 2019–20:

The QLD CCC identified corrections regarding access to telecommunications data for the 2018–19 and 2019–20 reporting periods. The below details both the original figures provided for the 2018–19 and 2019–20 Annual Reports and the amended figures as identified and corrected.

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

Agency	Authorisations			
	18/19 Original	18/19 Updated	19/20 Original	19/20 Updated
QLD CCC	1,009	1,039[60]	710	730[61]
TOTAL	**289,637**	**289,667**	**306,995**	**307,018**[62]

Prospective data authorisations – paragraph 186(1)(c) [63]

	Number of authorisations made			
Agency	18/19 Original	18/19 Updated	19/20 Original	19/20 Updated
QLD CCC	210	225	152	174
TOTAL	**27,771**	**27,950**[64]	**32,856**	**32,934**[65]

[59] Correction refers to Table 27, page 42, 2017-18 TIA Act Annual Report.
[60] Correction refers to Table 30, page 54, 2018-19 TIA Act Annual Report and Appendix D, page 89, 2019-20 TIA Act Annual Report.
[61] Correction refers to Table 29, page 56, 2019-20 Annual Report.
[62] This total figure includes updates from Home Affairs which are identified within this Appendix.
[63] 2018-19 corrections refer to Table 33, page 57, 2018-19 TIA Act Annual Report and Appendix D, page 90, 2019-20 TIA Act Annual Report. 2019-20 corrections refer to Table 32, page 60, 2019-20 TIA Act Annual Report.
[64] This total figure includes updates from the AFP which are identified in this Appendix.
[65] These total figures include updates from the AFP and Home Affairs which are identified in this Appendix.

Average specified and actual time in force of prospective data authorisations[66]

Agency	Average period specified		Average period actual	
	18/19 Original	18/19 Updated	18/19 Original	18/19 Updated
QLD CCC	41	43	31	36

Agency	Average period specified		Average period actual	
	19/20 Original	19/20 Updated	19/20 Original	19/20 Updated
QLD CCC	39	42	31	38

Offences for which authorisations were made under section 178 to access existing data to enforce the criminal law – paragraph 186(1)(e)[67]

Categories of offences	18/19 Original	18/19 Updated	19/20 Original	19/20 Updated
Abduction	-	-	3	3
Bribery or corruption	79	54	-	-
Fraud	310	62	445	37
Illicit drug offences	586	605	184	186
Miscellaneous	28	312	79	504
Weapons	6	6	-	-
TOTAL (QLD CCC)	**1,009**	**1,039**	**711**	**730**

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)[68]

Categories of offences	18/19 Original	18/19 Updated	19/20 Original	19/20 Updated
Abduction	-	-	3	4
Bribery or corruption	93	7	11	13
Fraud	6	6	76	79
Illicit drug offences	111	114	35	45
Miscellaneous	-	98	26	33
TOTAL	**210**	**225**	**151**	**174**

Periods which retained data was held by carrier before authorised disclosure – paragraph 186(1)(f)[69]

QLD CCC	Age of disclosure									
	0 – 3 mths	3 – 6 mths	6 – 9 mths	9 – 12 mths	12 – 15 mths	15 – 18 mths	18 – 21 mths	21 – 24 mths	Over 24 mths	TOTAL
18/19 Original	607	152	75	52	27	33	8	3	57	**1,014**

[66] 2018-19 corrections refer to Table 34, page 58, 2018-19 TIA Act Annual Report. 2019-20 corrections refer to Table 33, pages 61, 2019-20 TIA Act Annual Report.
[67] 2018-29 corrections refer to Table 35, page 61-2, 2018-29 TIA Act Annual Report. 2019-20 corrections refer to Table 34, pages 63-4, 2019-20 TIA Act Annual Report.
[68] 2018-19 corrections refer to Table 38, pages 67-8, 2018-19 TIA Act Annual Report. 2019-20 corrections refer to Table 37, pages 69-70, 2019-20 TIA Act Annual Report.
[69] 2018-19 corrections refer to Table 39, page 70, 2018-19 TIA Act Annual Report. 2019-20 corrections refer to Table 38, page 72, 2019-20 TIA Act Annual Report.

QLD CCC	Age of disclosure									
	0 – 3 mths	3 – 6 mths	6 – 9 mths	9 – 12 mths	12 – 15 mths	15 – 18 mths	18 – 21 mths	21 – 24 mths	Over 24 mths	TOTAL
18/19 Updated	721	103	64	51	23	22	8	4	48	**1,044**
19/20 Original	626	56	36	23	49	9	4	2	58	**863**
19/20 Updated	486	59	44	21	49	7	7	-	58	**731**

Types of retained data disclosed in authorisations – paragraphs 186(1)(g) and 186(1)(h)[70]

QLD CCC	Item 1: subscriber data	Items 2 – 6: traffic data
18/19 Original	750	264
18/19 Updated	778	266
19/20 Original	658	205
19/20 Updated	524	207

TAS Police 2019–20:

TAS Police identified corrections regarding applications for stored communications warrants for the 2019-20 reporting period. The additional warrants were not included in the original figures as the preservation notices were made during the 2018-19 reporting period. The increase in arrest increased due to the additional warrants being included in the figures. The below details both the original figures provided for the 2019–20 Annual Report and the amended figures as identified and corrected.

Applications, telephone applications and renewal applications for stored communications warrants – paragraphs 162(1)(a)-(b) and 162(2)(a)-(c)[71]

Agency	Relevant statistics	Applications for stored communications warrants	
		19/20 Original	19/20 Updated
TAS Police	Made	28	36
	Refused	-	-
	Issued	28	36
TOTAL[72]	**Made**	**1,385**	**1,394**
	Refused	**-**	**-**
	Issued	**1,385**	**1,394**

[70] 2018-19 corrections refer to Table 40, page 71, 2018-19 TIA Act Annual Report. 2019-20 corrections refer to Table 39, page 73, and 2019-20 TIA Act Annual Report.
[71] Correction refers to Table 23, pages 47-8, 2019-20 TIA Act Annual Report.
[72] This total figure includes updates from WA Police which are identified in this Appendix.

Stored Communications warrants subject to conditions or restrictions – paragraph 162(2)(d)[73]

Agency	19/20 Original	19/20 Updated
TAS Police	-	4
TOTAL	866	870

Number of arrests, proceedings, and convictions made on the basis of lawfully accessed information – paragraphs 163(a)-(b)[74]

Agency	Arrests	
	19/20 Original	19/20 Updated
TAS Police	15	18
TOTAL	542	545

WA Police 2019-20

WA Police identified corrections regarding applications for stored communications warrants for the 2019-20 reporting period. The below details both the original figures provided for the 2019–20 Annual Report and the amended figures as identified and corrected.

Applications, telephone applications and renewal applications for stored communications warrants – paragraphs 162(1)(a)-(b) and 162(2)(a)-(c)[75]

Agency	Relevant statistics	Applications for stored communications warrants	
		19/20 Original	19/20 Updated
WA Police	Made	103	104
	Refused	-	-
	Issued	103	104
TOTAL[76]	**Made**	**1,385**	**1,394**
	Refused	**-**	**-**
	Issued	**1,385**	**1,394**

[73] Correction refers to Table 24, page 49, 2019-20 TIA Act Annual Report.
[74] Correction refers to Table 25, page 50, 2019-20 TIA Act Annual Report.
[75] Correction refers to Table 23, pages 47-8, 2019-20 TIA Act Annual Report.
[76] This total figure includes updates from TAS Police which are identified in this Appendix.

APPENDIX E – CATEGORIES OF OFFENCES ABBREVIATIONS

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

APPENDIX F – RETAINED DATA SETS

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

Item	Description of information	Explanation
2. The source of a communication	Identifiers of a related account, service or device from which a communication has been sent or attempted to be sent by means of the relevant service.	Identifiers for the source of a communication may include, but are not limited to: • the phone number, IMSI, IMEI from which a call or SMS was made • identifying details (such as username, address, number) of the account, service or device from which a text, voice, or multi-media communication was made (examples include email, Voice over IP (VoIP), instant message or video communication) • the IP address and port number allocated to the subscriber or device connected to the internet at the time of the communication, or • any other service or device identifier known to the provider that uniquely identifies the source of the communication. In all instances, the identifiers retained to identify the source of the communication are the ones relevant to, or used in, the operation of the particular service in question.

Item		Description of information	Explanation
3.	**The destination of a communication**	Identifiers of the account, telecommunications device or relevant service to which the communication: a) has been sent; or b) has been forwarded, routed or transferred, or attempted to be forwarded, routed or transferred.	Paragraph 187A(4)(b) puts beyond doubt that service providers are not required to keep information about subscribers' web browsing history. The destination of a communication is the recipient. Identifiers for the destination of a communication may include, but are not limited to: • The phone number that received a call or SMS. • Identifying details (such as username, address, or number) of the account, service, or device which receives a text, voice, or multi-media communication (example include email, VoIP, instant message or video communication). • The IP address allocated to a subscriber or device connected to the internet at the time of receipt of the communication. • Any other service or device identifier known to the provider that uniquely identifies the destination of the communication. For internet access services, the Bill explicitly excludes anything that is web-browsing history or could amount to web-browsing history, such as a URL or IP address to which a subscriber has browsed. In all instances, the identifiers retained to identify the destination of the communications are the ones relevant to, or used in, the operation of the particular service in question. If the ultimate destination of a communication is not feasibly available to the provider of the service, the provider must retain only the last destination knowable to the provider.
4.	**The date, time and duration of a communication, or of its connection to a relevant service**	The date and time (including the time zone) of the following relating to the communication (with sufficient accuracy to identify the communication): a) the start of the communication b) the end of the communication c) the connection to the relevant service, and d) the disconnection from the relevant service.	For phone calls this is simply the time a call started and ended. For internet sessions this is when a device or account connects to a data network and ends when it disconnected – those events may be a few hours to several days, weeks, or longer apart, depending on the design and operation of the service in question.

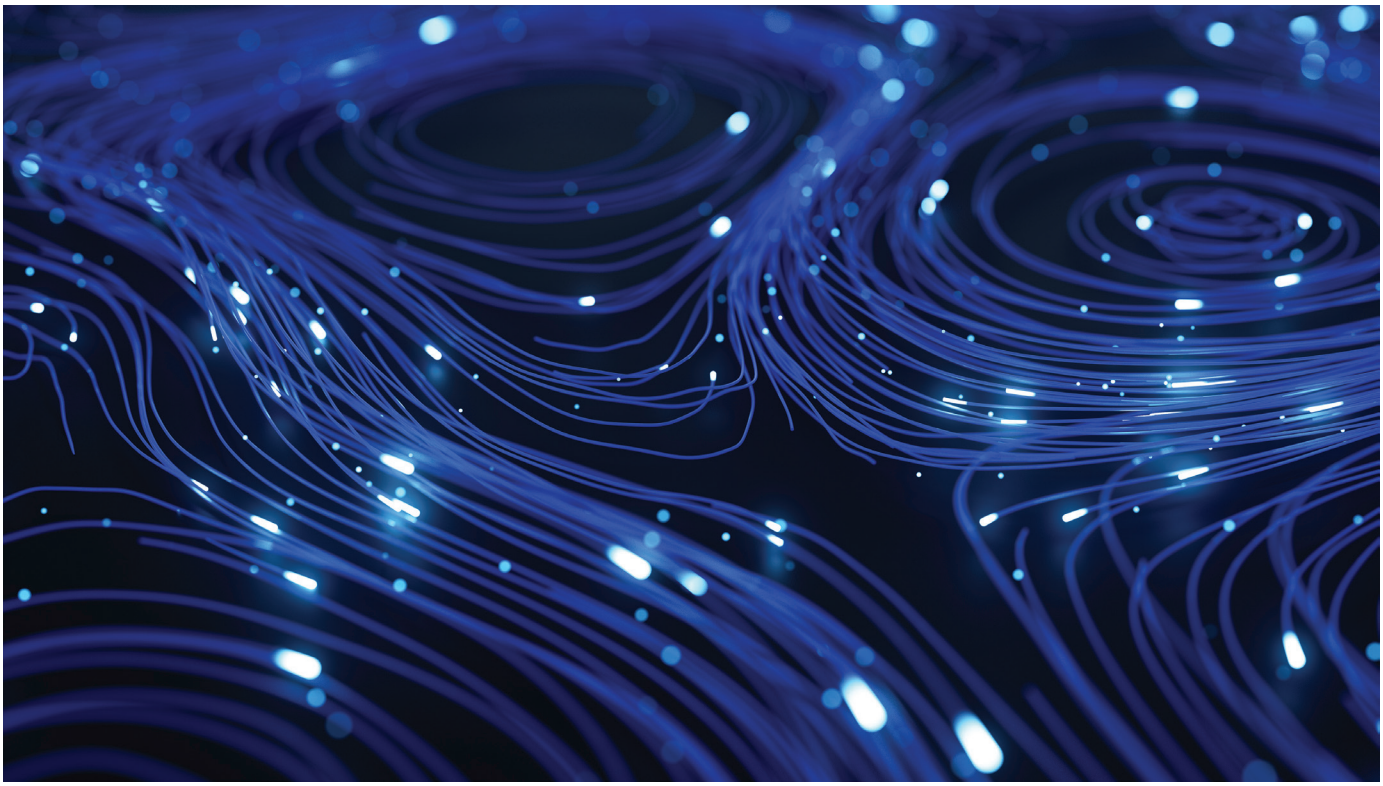
	Item	Description of information	Explanation
5.	**The type of communication and relevant service used in connection with a communication**	The following: a) the type of communication; Examples: Voice, SMS, email, chat, forum, social media. b) the type of the relevant service; Examples: ADSL, Wi-Fi, VoIP, cable, GPRS, VoLTE, LTE. c) the features of the relevant service that were, or would have been, used by or enable for the communication. Examples: call waiting, call forwarding, data volume usage.	The type of communication means the form of the communication (for example voice call vs. internet usage). The type of the relevant service (see 5(b) at left) provides more technical detail about the service. For example, for a mobile messaging service, whether it is an SMS or MMS. Data volume usage, applicable to internet access services, refers to the amount of data uploaded and downloaded by the subscriber. This information can be measured for each session, or in a way applicable to the operation and billing of the service in question, such as per day or per month. Note: This item will only apply to the service provider operating the relevant service: see paragraph 187A(4)(c).
6.	**The location of equipment or a line used in connection with a communication**	The following in relation to the equipment or line used to send or receive the communication: a) the location of the equipment or line at the start of the communication; b) the location of the equipment or line at the end of the communication. Examples: Cell towers, Wi-Fi hotspots.	Location records are limited to the location of a device at the start and end of a communication, such as a phone call or Short Message Service (SMS) message. For services provided to a fixed location, such as an ADSL service, this requirement can be met with the retention of the subscriber's address. Paragraph 187(4)(e) of the TIA Act provides that location records are limited to information that is used by a service provider in relation to the relevant service. This would include information such as which cell tower, Wi-Fi hotspot or base station a device was connected to at the start and end of communication. Service providers are not required to keep continuous, real-time, or precise location records, such as the continuous GPS location of a device. These limitations seek to ensure that the location records to be kept by service providers do not allow continuous monitoring or tracking of devices.

APPENDIX G – DESIGNATED COMMUNICATIONS PROVIDERS

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

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

NOTES



www.homeaffairs.gov.au