Australian Government
Department of Home Affairs

Telecommunications (Interception and Access) Act 1979

Annual Report 2017–18

ISSN: 1035-1949 (Print)
ISSN: 2652-1652 (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 2017 – 18

THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY

Table of Contents

EXECUTIVE SUMMARY

The *Telecommunications (Interception and Access) Act 1979 Annual Report 2017–18* sets out the extent and circumstances in which eligible Commonwealth, State, and Territory government agencies have used the powers available under the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) between 1 July 2017 – 30 June 2018.

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

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

Legislative reforms

National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018

The *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* amended the definition of 'serious offence' in the TIA Act to include new *Criminal Code Act 1995* offences relating to espionage and foreign interference. This amendment ensures law enforcement and intelligence agencies are able to take reasonable steps to detect, disrupt, investigate, and prosecute those suspected of engaging in such conduct.

Investigation and Prosecution Measures Act 2018

The *Investigation and Prosecution Measures Act 2018* made minor amendments to the TIA Act to reflect the restructuring of the Independent Commission against Corruption of New South Wales (ICAC NSW) by the *Independent Commission Against Corruption Amendment Act 2016* (NSW). The Act made no substantive changes to ICAC NSW's powers under the TIA Act.

Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018

The *Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018* amended the TIA Act to ensure Australia can effectively respond to requests from the International Criminal Court (ICC) and international war crimes tribunals (IWCT). The amendments allow Australia to provide lawfully obtained information under the TIA Act to, and receive requests from, the ICC and IWCT for investigating and prosecuting offences within their jurisdiction.

Home Affairs and Integrity Agencies Legislation Amendment Act 2018

The *Home Affairs and Integrity Agencies Legislation Amendment Act 2018* amended 36 Acts including the TIA Act, to make Ministerial and Departmental functions and powers clear on the face of legislation as a result of the Machinery of Government changes to establish the Home Affairs portfolio, and made changes strengthening the Attorney-General's oversight of intelligence, security, and law enforcement agencies.

Telecommunications and Other Legislation Amendment Act 2017

The *Telecommunications and Other Legislation Amendment Act 2017* amended the TIA Act, and several other pieces of legislation (most notably the *Telecommunications Act 1997)*, in order to introduce a regulatory framework to manage national security risks of espionage, sabotage and foreign interference to Australia's telecommunications networks and facilities.

Carriers, carriage service providers, and carriage service intermediaries are now required to protect telecommunications networks and facilities they own, operate, or use from unauthorised interference and access, and protect the confidentiality of information stored on, and carried across them. Certain providers must also notify the Government of planned changes to systems and services that are likely to make the network or facility vulnerable to unauthorised access and interference.

Key judicial decisions

No significant judicial decisions relevant to the TIA Act occurred during the reporting period.

Key findings

The following key statistics are relevant to the 2017–18 reporting period.

- 3,524 interception warrants were issued.
- Information obtained under interception warrants was used in:[1]
    - 2,429 arrests;[2]
    - 5,415 prosecutions; and
    - 3,516 convictions.
- 20 enforcement agencies made 301,113 authorisations for the disclosure of historical telecommunications data – an increase of 889 authorisations from the previous reporting period. Of these, 295,779 were made to enforce a criminal law.
- The majority of criminal law offences for which historical data was requested were illicit drug offences (67,621 requests), followed by 33,261 requests for homicide and related offences and 21,305 requests for fraud.
- Law enforcement agencies made 412 arrests, conducted 611 proceedings, and obtained 356 convictions based on evidence obtained under stored communications warrants.[3]

[1] These figures provide an indication about the effectiveness of interception rather than the full picture as, for example, a conviction can be recorded without admitting intercepted information into evidence.
[2] This figure includes the number of times lawfully intercepted information culminated in an arrest.
[3] These figures provide an indication about the effectiveness of stored communications rather than the full picture as, for example, a conviction can be recorded without admitting stored communications into evidence.

Access to the content of a communication

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

Accessing communications is an effective investigative tool that supports and complements information obtained by other methods. In some cases, the weight of evidence obtained by either an interception or a stored communications warrant results in defendants entering guilty pleas, thereby eliminating the need for the intercepted information to be introduced into evidence.

Telecommunications data

A critical tool available under the TIA Act is access to telecommunications data.[4]

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

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

Access to telecommunications data is regulated by Chapter 4 of the TIA Act, which permits an authority or body that is an 'enforcement agency' under the TIA Act to authorise telecommunications carriers to disclose telecommunications data where that information is reasonably necessary for the enforcement of the criminal law, a law imposing a pecuniary penalty, or the protection of the public revenue.

During the 2017–18 reporting period all enforcement agencies could access historical data[5] and only criminal law enforcement agencies could access prospective data to assist in the investigation of offences punishable by at least three year's imprisonment.[6] The *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015*, passed by the Parliament in March 2015, reduced the number of enforcement agencies that may access

[4] Telecommunications data is information about a communication such as the phone numbers of the people who called each other, how long they talked to each other, the email address from which a message was sent, and the time the message was sent.
[5] Historical data, also known as existing data, is information that is already in existence when an authorisation for disclosure is received by a telecommunications carrier.
[6] Prospective data is telecommunications data that comes into existence during a period of time in which an authorisation is in force.

telecommunications data to 20 specified agencies. The Minister may declare additional agencies in prescribed circumstances. No additional agencies were prescribed in the 2017–18 reporting period.

Format of Annual Report

The Annual Report is organised into three main chapters:

- Chapter 1 – telecommunications interception;
- Chapter 2 – stored communications; and
- Chapter 3 – telecommunications data.

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

More information

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

- Department of Home Affairs <www.homeaffairs.gov.au>
- Attorney-General's Department <www.ag.gov.au>
- Department of Communications and the Arts <www.communications.gov.au>
- Commonwealth Ombudsman <www.ombudsman.gov.au>
- Office of the Australian Information Commissioner <www.oaic.gov.au>
- Telecommunications Industry Ombudsman <www.tio.com.au>
- Australian Communications and Media Authority <www.acma.gov.au>

CHAPTER 1 – TELECOMMUNICATIONS INTERCEPTION

The primary function of the TIA Act is to protect the privacy of the communications of people who use the Australian telecommunications network by making it an offence to intercept communications, subject to limited lawful exceptions. The TIA Act prohibits communications from being intercepted while they are passing over an Australian telecommunications system, except as authorised under the circumstances set out in the TIA Act.

Definition

The term **'interception agency'** is defined in section 5 of the TIA Act. An interception agency is limited to bodies such as the AFP and state and territory police forces. Only defined interception agencies are eligible to apply under Part 2-5 of the TIA Act for an interception warrant.

The TIA Act provides for several types of warrant that enable access to real-time content (for example, a phone call while the parties are talking with each other). During the reporting period, interception warrants were available to 17 Commonwealth, state, and territory agencies including:

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

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

Serious offences

Interception warrants can only be obtained to investigate serious offences. Serious offences generally carry a penalty of at least seven years imprisonment.[7]

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

The information provided in Table 1 illustrates the important role telecommunications interception plays in investigating serious crimes. Consistent with previous years, in 2017–18 the majority of warrants obtained were to assist with investigations into serious drug offences (1,904 warrants). Loss of life or personal injury offences were specified in 656 warrants and 372 related to murder investigations. Money laundering was specified as an offence in 294 warrants. The total number of offences is typically larger than the total number of warrants issued, as a warrant can be issued to investigate more than one serious offence.

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

[7] There are exceptions to this threshold. Interception warrants may be available for offences that typically involve the use of the telecommunications system, such as offences involving collusion. In these circumstances telecommunications interception is a critical investigative tool and its availability may be key to resolving an investigation.

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

Categories of offences	ACIC	ACLEI	AFP	CCC (QLD)	CCC (WA)	IBAC	ICAC (NSW)	ICAC (SA)	LECC	NSW CC	NSW Police	NT Police	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
ACIC special investigations	105	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**105**
Administration of justice	-	16	15	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**31**
Bribery, corruption and dishonesty offences	-	3	26	36	36	18	4	7	4	-	8	1	3	-	-	-	29	**175**
Cartel offences	-	-	6	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**6**
Child pornography offences	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	6	**7**
Conspire/aid/abet serious offence	-	-	1	-	-	-	-	4	-	13	4	-	5	1	-	1	-	**29**
Cybercrime offences	-	-	8	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**8**
Kidnapping	-	-	-	-	-	-	-	-	-	8	38	-	-	-	-	9	-	**55**
Loss of life or personal injury	-	-	126	-	-	-	-	-	-	4	425	-	25	2	1	54	19	**656**
Money laundering	72	-	145	3	-	-	-	-	-	66	-	-	-	5	-	3	-	**294**
Murder	-	-	17	-	-	-	-	-	-	15	226	2	31	11	3	32	35	**372**
Organised offences and/or criminal organisations	-	-	15	-	-	-	-	-	-	11	30	-	-	-	3	3	4	**66**
People smuggling and related	-	-	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**2**
Serious damage to property and/or serious arson	-	-	-	-	-	-	-	-	-	-	39	-	1	-	-	10	13	**63**
Serious drug offences and/or trafficking	149	6	542	11	-	3	-	-	2	46	580	27	190	47	10	79	212	**1,904**
Serious fraud	-	-	23	-	-	4	12	-	8	12	51	-	10	5	3	5	2	**135**
Serious loss of revenue	-	-	16	-	-	-	-	-	-	-	1	-	-	-	-	-	-	**17**
Telecommunications offences	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**0**
Terrorism financing offences	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**1**
Terrorism offences	-	-	109	-	-	-	-	-	-	-	11	-	-	-	-	-	-	**120**
TOTAL	**327**	**25**	**1,052**	**50**	**36**	**25**	**16**	**11**	**14**	**175**	**1,413**	**30**	**265**	**71**	**20**	**196**	**320**	**4,046**

Eligibility to issue an interception warrant

An interception warrant may only be issued by an eligible judge, or a nominated Administrative Appeals Tribunal (AAT) member. Table 2 records that, as of December 2018, there were 91 issuing authorities.

An eligible judge is a judge who has consented in writing and been declared by the Attorney-General to be an eligible judge. In the reporting period, eligible judges included members of the:

- Federal Court of Australia
- Family Court of Australia
- Federal Circuit Court

Table 2: Number of Federal Court Judges, Family Court Judges, Federal Circuit Court Judges and nominated AAT members to issue telecommunications interception warrants as of December 2018 – subsection 103(ab)

Issuing Authority	Number eligible
Federal Court judges	14
Family Court judges	6
Federal Circuit Court judges	32
Nominated AAT members	39

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

- the gravity of the conduct of the offence/s being investigated;
- how much the interception would be likely to assist with the investigation; and
- the extent to which other methods of investigating the offence are available to the agency.

Applications for and issue of telecommunications interception warrants

Table 3 sets out information stating which authorities issued warrants to each of the interception agencies in the reporting period. In 2017-18 issuing authorities issued 3,524 interception warrants, a decrease from 2016-17, when 3,717 warrants were issued.

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

Agency	Issuing Authority			
	Family Court judges	Federal Circuit Court judges	Federal Court judges	Nominated AAT members
ACIC	45	23	-	118
ACLEI	-	6	-	10
AFP	29	51	2	642
CCC (QLD)	-	7	-	43
CCC (WA)	33	-	2	1
IBAC	-	-	-	25
ICAC (NSW)	-	1	-	15
ICAC (SA)	-	4	-	7
LECC	-	-	4	13
NSW CC	-	-	-	135
NSW Police	-	71	1	1,338
NT Police	-	30	-	-
QLD Police	-	245	-	29
SA Police	-	7	-	51
TAS Police	-	-	-	20
VIC Police	-	-	-	196
WA Police	228	-	-	92
TOTAL	**335**	**445**	**9**	**2,735**

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

Agency	Relevant Statistics	Applications for warrants		Telephone applications for warrants		Renewal applications	
		16 / 17	17 / 18	16 / 17	17 / 18	16 / 17	17 / 18
ACIC	Made	242	186	-	-	33	21
ACLEI	Made	27	16	-	-	13	7
AFP	Made	904	724	-	2	312	246
	Refused	1	-	-	-	-	-
CCC (QLD)	Made	44	50	-	-	17	8
	Refused	2	-	-	-	-	-
CCC (WA)	Made	37	36	-	-	7	13
IBAC	Made	13	26	-	-	4	9
	Refused	-	1	-	-	-	1
ICAC (NSW)	Made	5	16	-	-	2	7
ICAC (SA)	Made	26	11	-	-	2	-
	Refused	1					
LECC	Made	2	17	-	-	-	5
NSW CC	Made	150	135	-	-	54	49
NSW Police	Made	1,499	1,413	18	39	325	309
	Refused	-	3	-	-	-	-
NT Police	Made	31	31	-	-	2	-
	Refused	-	1	-	-	-	-
QLD Police	Made	251	274	-	-	37	43
SA Police	Made	65	58	-	-	3	3
TAS Police	Made	30	20	-	-	-	1
VIC Police	Made	189	196	4	11	18	20
WA Police	Made	206	320	-	-	13	22
TOTAL	**Made**	**3,721**	**3,529**	**22**	**52**	**842**	**763**
	Refused	**4**	**5**	**-**	**-**	**-**	**1**
	Issued	**3,717**	**3,524**	**22**	**52**	**842**	**762**

Warrants that authorise entry on to premises

The TIA Act provides that in exceptional circumstances, an issuing authority can issue an interception warrant that authorises entry on to premises to carry out telecommunications interception. An issuing authority can only issue such a warrant if satisfied that it would be impracticable or inappropriate to intercept communications otherwise than by use of equipment installed on those premises. Agencies only use this type of warrant on rare occasions. There were no warrants issued in the 2017–18 period that authorised entry on to premises.

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

Agency	Relevant statistics	Warrants authorising entry on premises	
		16 / 17	17 / 18
AFP	Made	1	-
	Refused/Withdrawn	-	-

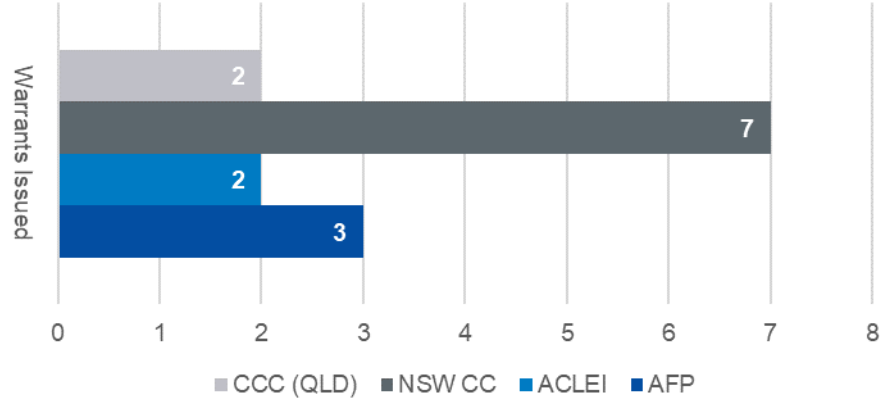
Conditions or restrictions on warrants

Issuing authorities can place any conditions or restrictions on an interception warrant they consider necessary. 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.

During the reporting period, 14 interception warrants were issued with a condition or restriction.

Figure 1 provides information about how these warrants are distributed across interception agencies.

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



Effectiveness of telecommunications interception warrants

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

The tables may understate the effectiveness of interception, 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.

In 2017–18 there were 3,423 arrests based on lawfully intercepted information (this figure includes instances where lawfully intercepted information culminated in an arrest). There were also 5,415 prosecutions and 3,516 convictions where lawfully intercepted material was given in evidence. Tables 6, 7 and 8 provide this information.

Agencies have been asked to report on the number of times lawfully intercepted information culminated in an arrest separately from arrest numbers. This change removes the risk that arrest numbers will be duplicated. This change also shows outcomes from agencies that do not have arrest powers.

Table 6: Arrests on the basis of lawfully intercepted information – paragraphs 102(1)(a) and 100(2)(e)

Agency	2016 / 2017		2017 / 2018	
	Number of arrests	Number of times lawfully intercepted information culminated in arrest	Number of arrests	Number of times lawfully intercepted information culminated in arrest
ACIC	-	115	-	99
ACLEI	1	1	2	2
AFP	100	84	165	100
CCC (QLD)	33	8	39	10
IBAC	-	1	-	2
ICAC (NSW)	-	-	-	-
ICAC (SA)	5	5	-	-
NSW CC	-	49	-	70
NSW Police	1,165	-	763	-
NT Police	37	11	45	45
QLD Police	429	-	606	-
SA Police	63	-	46	5
TAS Police	21	21	15	15
VIC Police	283	66	337	70
WA Police	357	497	411	576
TOTAL	**2,494**	**858**	**2,429**	**994**

Table 7: Prosecutions per offence category in which lawfully intercepted information was given in evidence

Category	ACIC	ACLEI	AFP	CCC (QLD)	IBAC	LECC	NSW CC	NSW Police	NT Police	QLD Police	SA Police	VIC Police	WA Police	TOTAL
ACIC special investigations	-	-	-	-	-	-	-	-	-	-	-	-	-	**-**
Assisting person to escape or dispose of proceeds	-	-	2	-	-	-	7	-	-	1	1	-	-	**11**
Bribery or corruption	-	-	1	3	5	-	-	-	-	-	-	-	17	**26**
Child pornography offences	-	-	7	-	-	-	-	-	-	-	-	-	9	**16**
Conspire/aid/abet serious offence	-	-	5	-	-	-	-	-	-	1	-	3	-	**9**
Kidnapping	-	-	7	-	-	-	-	5	-	-	-	5	-	**17**
Loss of life	-	-	-	-	-	-	-	-	-	4	-	2	3	**9**
Money laundering	-	-	-	-	-	-	89	-	-	1	-	40	-	**130**
Murder	-	-	4	-	-	-	9	34	-	2	5	5	19	**78**
Offences involving planning and organisation	-	-	-	-	-	-	-	124	-	-	-	3	612	**739**
Organised crime	-	-	-	-	-	-	-	2	-	-	-	-	-	**2**
Other offence punishable by 3 years to life	-	11	2	-	-	-	-	51	-	54	-	80	-	**198**
People smuggling and related	-	-	15	-	-	-	-		-	-	-	-	-	**15**
Serious arson	-	-	-	-	-	-	-	9	-	-	-	4	7	**20**
Serious damage to property	-	-	2	-	-	-	1	-	-	-	-	-	14	**17**
Serious drug offence and/or trafficking	3	4	71	-		-	-	305	45	-	-	1	-	**429**
Serious fraud	-	-	28	-	5	2	20	165	-	1	-	1	5	**227**
Serious personal injury	-	-	1	-	-	-	1	25	-		1	12	7	**47**
Telecommunications offences	-	-	1	-	-	-	-	-	-	-	-	-	-	**1**
Terrorism offences	-	-	17	-	-	-	-	-	-	-	-	-	-	**17**
Trafficking in prescribed substances	-	-	11	15	4	-	120	115	-	244	43	158	2,697	**3,407**
Total	**3**	**15**	**174**	**18**	**14**	**2**	**247**	**835**	**45**	**308**	**50**	**314**	**3,390**	**5,415**

Table 8: Convictions per offence category in which lawfully intercepted information was given in evidence

Category	ACIC	ACLEI	AFP	CCC (QLD)	IBAC	NSW CC	NSW Police	NT Police	QLD Police	SA Police	VIC Police	WA Police	TOTAL
ACIC special investigations	-	-	-	-	-	-	-	-	-	-	-	-	**0**
Assisting person to escape or dispose of proceeds	-	-	-	-	-	2	-	-	1	-	-	-	**3**
Bribery or corruption	-	-	-	3	2	-	-	-	-	-	-	11	**16**
Child pornography offences	-	-	-	-	-	-	1	-	-	-	-	5	**6**
Conspire/aid/abet serious offence	-	-	2	-	-	-	-	-	1	-	3	-	**6**
Kidnapping	-	-	5	-	-	-	25	-	-	-	2	-	**32**
Loss of life	-	-	-	-	-	-	-	-	4	-	2	1	**7**
Money laundering	-	-	-	-	-	21	-	-	1	-	36	-	**58**
Murder	-	-	-	-	-	2	40	-	2	5	4	9	**62**
Offences involving planning and organisation	-	-	-	-	-	-	40	-	-	-	3	432	**475**
Organised crime	-	-	-	-	-	-	61	-	-	2	-	-	**63**
Other offence punishable by 3 years to life	-	5	1	-	-	-	24	-	39	-	77	-	**146**
People smuggling and related	-	-	4	-	-	-	-	-	-	-	-	-	**4**
Serious arson	-	-	1	-	-	-	8	-	-	-	3	3	**15**
Serious damage to property	-	-	2	-	-	-	-	-	-	-	-	9	**11**
Serious drug offence and/or trafficking	3	4	20	-	-	-	125	21	-	-	1	-	**174**
Serious fraud	-	-	6	-	5	7	55	-	-	-	1	2	**76**
Serious personal injury	-	-	1	-	-	-	31	-	-	-	9	4	**45**
Telecommunications offences	-	-	1	-	-	-	-	-	-	-	-	-	**1**
Terrorism offences	-	-	12	-	-	-	-	-	-	-	-	-	**12**
Trafficking in prescribed substances	-	-	2	6	4	77	75	-	159	43	140	1,798	**2,304**
Total	**3**	**9**	**57**	**9**	**11**	**109**	**485**	**21**	**207**	**50**	**281**	**2,274**	**3,516**

Named person warrants

A named person warrant can authorise the interception of multiple telecommunications services (such as a landline or mobile service), or in certain circumstances telecommunications devices (such as a mobile handset). Before issuing a named person warrant an issuing authority must take into account:

- how much the privacy of any person would be likely to be interfered with;
- the gravity of the 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.

The following tables and figures show that in 2017–18, 691 named person warrants were issued, a decrease from the 2016–17 reporting period in which 824 named person warrants were issued.

In 2017–18, five named person warrants were issued with a condition or restriction. Three were issued to the AFP, and two were issued to the NSW CC.

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)

Agency	Relevant Statistics	Applications for named person warrants		Telephone applications for named person warrants		Renewal applications for named person warrants	
		16 / 17	17 / 18	16 / 17	17 / 18	16 / 17	17 / 18
ACIC	Made	129	88		-	24	12
	Refused / Withdrawn	-	-	-	-	-	-
AFP	Made	323	245	-	-	120	79
	Refused / Withdrawn	1	-	-	-	-	-
CCC (QLD)	Made	14	7	-	-	6	1
CCC (WA)	Made	10	14	-	-	4	7
IBAC	Made	-	2	-	-	-	1
NSW CC	Made	87	67	-	-	25	33
NSW Police	Made	119	87	-	-	42	31
NT Police	Made	-	3	-	-	-	-
QLD Police	Made	42	56	-	-	5	5
SA Police	Made	5	4	-	-	-	-
TAS Police	Made	6	3	-	-	-	-
VIC Police	Made	59	52	-	1	12	8
WA Police	Made	31	63	-	-	2	4
Total	**Made**	**825**	**691**	**-**	**1**	**240**	**181**
	Refused / Withdrawn	**1**	**-**	**-**	**-**	**-**	**-**
	Issued	**824**	**691**	**-**	**1**	**240**	**181**

Consistent with previous reporting periods, in 2017–18 the majority of named person warrants were for the interception of between two to five telecommunications services.

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

Agency	Relevant statistics							
	1 service Only		2 – 5 services		6 – 10 services		10+ services	
	16 / 17	17 / 18	16 / 17	17 / 18	16 / 17	17 / 18	16 / 17	17 / 18
ACIC	28	27	94	53	5	3	-	1
AFP	133	68	175	158	10	13	3	-
CCC (QLD)	4	2	10	5	-	-	-	-
CCC (WA)	-	4	7	9	1	1	1	-
IBAC	-	-	-	2	-	-	-	-
NSW CC	47	25	36	34	2	8	-	-
NSW Police	35	16	74	35	8	6	2	-
NT Police	-	-	-	2	-	1	-	-
QLD Police	16	17	22	38	2	1	-	-
SA Police	2	-	3	4	-	-	-	-
TAS Police	1	1	4	2	1	-	-	-
VIC Police	13	5	35	45	10	2	1	-
WA Police	13	18	17	42	1	3	-	-
TOTAL	**292**	**183**	**477**	**429**	**40**	**38**	**7**	**1**

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) requires the report to include the total number of:

i. services intercepted under service based named warrants;
ii. services intercepted under device based named person warrants; and
iii. telecommunications devices intercepted under device based named person warrants

Figure 2 and Table 11 outline the number of services intercepted under the different types of named person warrants and should be read in conjunction with Table 9, which provides the total number of named person warrants issued.

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

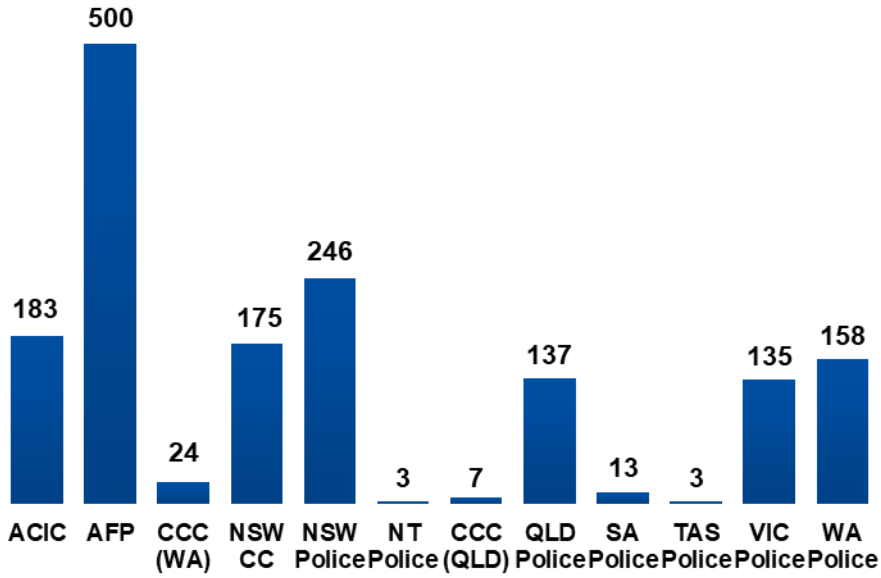


Table 11 shows that in 2017–18, device based named person warrants were used by only a small number of agencies. This is consistent with the 2016–17 reporting period.

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

Agency	Devices	Services
ACIC	5	16
AFP	66	-
NSW Police	23	87
VIC Police	2	6
TOTAL	**96**	**109**

B-Party warrants

Definition

A **'B-Party warrant'** is a 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. Table 12 shows that in 2017–18, 152 B-Party warrants were issued. This represents an increase on the 139 B-Party warrants issued in 2016–17.

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

Agency	Relevant Statistics	Applications for B-Party Warrants		Telephone applications for B-Party warrants		Renewal applications for B-Party warrants	
		16 / 17	17 / 18	16 / 17	17 / 18	16/17	17/18
ACIC	Made	1	-	-	-	-	-
AFP	Made	102	113	-	-	79	76
CCC (WA)	Made	2	-	-	-	-	-
NSW CC	Made	1	4	-	-	-	2
NSW Police	Made	29	30	3	10	2	2
QLD Police	Made	1	5	-	-	-	2
VIC Police	Made	3	-	-	-	-	-
TOTAL	**Made**	**139**	**152**	**3**	**10**	**81**	**82**
	Refused	**-**	**-**	**-**	**-**	**-**	**-**
	Issued	**139**	**152**	**3**	**10**	**81**	**82**

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

Agency	B-party warrants specifying conditions or restrictions	
	16 / 17	17 / 18
NSW Police	-	1
TOTAL	**-**	**1**

Duration of warrants

Under the TIA Act, a telecommunications interception warrant, other than a B-Party warrant, can be in force for up to 90 days. Under section 57, the chief executive of an agency may revoke a warrant at any time and must revoke a warrant if they are satisfied that the conditions for issuing the warrant no longer exist. Table 14 sets out the average length of time for which interception warrants – including renewals, but not including B-Party warrants – were issued and the average length of time they were in force in the reporting period.

Table 14: Duration of original and renewal telecommunications interception warrants – subparagraphs 101(1)(a)-(d) and 101(2)(a)-(d)

Agency	Duration of original telecommunications warrants		Duration of renewal telecommunications interception warrants	
	Average period specified in warrants (days)	Average period warrants in force (days)	Average period specified in warrants (days)	Average period warrants in force (days)
ACIC	87	62	88	61
ACLEI	77	47	90	88
AFP	80	80	74	67
CCC (QLD)	69	75	67	43
CCC (WA)	90	77	90	80
IBAC	83	79	79	72
ICAC (NSW)	90	85	90	88
ICAC (SA)	85	47	-	-
LECC	80	79	74	61
NSW CC	79	54	66	70
NSW Police	52	43	58	51
NT Police	89	55	-	-
QLD Police	79	53	75	60
SA Police	85	75	74	70
TAS Police	68	75	90	90
VIC Police	77	57	73	50
WA Police	78	48	90	49
AVERAGE	**79**	**64**	**79**	**67**

A single B-Party warrant can be in force for up to 45 days. Table 15 sets out the average periods of effect for B-Party warrants, inclusive of an average of the total time all renewals were in effect for a warrant.

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

Agency	Duration of original telecommunications B-party warrants		Duration of renewal telecommunications B-party warrants	
	Average period specified in warrants (days)	Average period warrants in force (days)	Average period specified in warrants (days)	Average period warrants in force (days)
AFP	46	34	45	44
NSW CC	45	44	45	40
NSW Police	29	13	28	28
QLD Police	25	25	15	15
AVERAGE	**36**	**29**	**33**	**32**

A final renewal means a telecommunications interception warrant that is the last renewal of an original warrant. A final renewal is recorded as the number of days after the issue of the original warrant. The categories of final renewals are:

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

Table 16 provides information on the number of final renewals used by agencies.

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

Agency	90 days		150 days		180 days	
	16 / 17	17 / 18	16 / 17	17 / 18	16/ 17	17 / 18
ACIC	5	6	11	2	9	7
ACLEI	-	-	-	1	-	2
AFP	20	32	65	17	81	73
CCC (QLD)	5	6	4	1	1	1
CCC (WA)	2	1	-	7	-	4
IBAC	1	3	3	2	-	-
ICAC (NSW)	1	-	1	4	-	-
LECC	-	1	-	-	-	2
NSW CC	1	2	4	4	4	4
NSW Police	137	116	17	12	39	25
NT Police	2	-	-	-	-	-
QLD Police	9	14	11	7	4	7
SA Police	1	3	-	-	-	-
VIC Police	13	11	3	-	1	3
WA Police	2	8	6	-	5	1
TOTAL	**199**	**203**	**125**	**57**	**144**	**129**

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.

Table 17 sets out the number of eligible warrants issued to agencies during the reporting period and the percentage of warrants issued to agencies that were eligible warrants.

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

Agency	Total number of warrants	Number of eligible warrants	%
ACIC	215	112	52
ACLEI	23	7	30
AFP	855	494	58
CCC (QLD)	60	29	48
CCC (WA)	49	-	0
IBAC	29	12	41
ICAC (NSW)	16	11	69
ICAC (SA)	13	4	31
LECC	17	8	47
NSW CC	159	120	75
NSW Police	1,547	1,146	74
NT Police	36	14	39
QLD Police	314	301	96
SA Police	71	54	76
TAS Police	20	7	35
VIC Police	224	98	44
WA Police	303	165	54
TOTAL / AVERAGE	**3,951**	**2,582**	**51%**

Interception without a warrant

Agencies can undertake interception without a warrant in limited circumstances. Table 18 reports on interceptions under subsection 7(5) of the TIA Act. There were no cases where an officer of the agency undertaking the interception was a party to the conversation.

Table 18: Interception without a warrant where a person consents – section 102A

Agency	Consent where person likely to receive communication from person who has:							
	Committed an act that has or may result in loss of life or serious personal injury		Threatened to kill or seriously injure another		Threatened to cause serious damage to property		Threatened to take, endanger, or create serious threat to own life/safety	
	16 / 17	17 / 18	16 / 17	17 / 18	16 / 17	17 / 18	16 / 17	17 / 18
NSW Police	4	-	-	1	-	-	-	-
TOTAL	**4**	**-**	**-**	**1**	**-**	**-**	**-**	**-**

Mutual assistance

Section 102B of the TIA Act requires that the annual report include information about the number of occasions on which lawfully intercepted or interception warrant information was provided to a foreign country under subsection 68(1) or section 68A of the TIA Act in connection with an authorisation under subsection 13A(1) of the *Mutual Assistance in Criminal Matters Act 1987* (the Mutual Assistance Act). No authorisations were issued under section 13A during the reporting period that included interception material.

Number of interceptions carried out on behalf of other agencies

The TIA Act supports the ability of interception agencies to cooperate and to work collaboratively by enabling one interception agency to carry out interception on behalf of other agencies.

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

Interception carried out by:	Interception carried out on behalf of:	Number of interceptions
ACIC	ACLEI	1
	CCC (QLD)	47
AFP	ACLEI	16
IBAC	ICAC (SA)	11
	CCC (WA)	1
LECC	IBAC	3
	ICAC (SA)	1
VIC Police	TAS Police	19
TOTAL		**99**

Telecommunications interception expenditure

Table 20 below provides information about the total expenditure (including expenditure of a capital nature) by interception agencies on telecommunications interception warrants and the average expenditure (total warrant expenditure divided by the number of warrants issued) per warrant. The average cost per warrant is significantly affected by capital expenditure (which can vary significantly, for instance, due to a capital upgrade program) and the number of warrants issued, meaning that smaller interception agencies typically have higher average costs as they apply for fewer warrants. Care should be taken in comparing costs associated with average expenditure as interception agencies employ different interception models which may result in some costs associated with interception being delineated, and for other agencies, those same costs being included in their average expenditure.

Table 20: Total expenditure incurred by each agency in connection with the execution of telecommunications interception warrants and average expenditure per telecommunications interception warrant – subsections 103(a) and 103(aa).

Agency	Total expenditure ($)	Average expenditure ($)
ACIC	8,426,961	45,306
ACLEI	743,067	46,442
AFP	15,267,232	21,087
CCC (QLD)	1,734,682	34,694
CCC (WA)	942,435	26,179
IBAC	604,664	24,187
ICAC (NSW)	323,059	20,191
ICAC (SA)	159,058	14,460
LECC	828,484	48,734
NSW CC	2,141,197	15,861
NSW Police	10,871,480	7,710
NT Police	394,882	13,163
QLD Police	6,161,017	22,485
SA Police	3,450,380	53,083
TAS Police	809,013	40,496
VIC Police	1,248,867	6,372
WA Police	3,530,366	11,032
TOTAL / AVERAGE	**57,636,844**	**26,558**

Table 21 provides a breakdown of the total recurrent costs of interception over the reporting period. As agencies do not necessarily treat or record particular items of expenditure in the same way, caution should be exercised in comparing costs incurred by individual agencies.

Table 21: Recurrent interception costs per agency

Agency	Salaries	Administrative Support	Capital expenditure	Interception costs	Total ($)
ACIC	5,740,100	97,737	702,632	1,886,492	**8,426,961**
ACLEI	641,432	45,950	-	55,685	**743,067**
AFP	10,044,285	191,696	5,031,250	-	**15,267,231**
CCC (QLD)	1,134,617	140,587	52,484	406,994	**1,734,682**
CCC (WA)	626,381	15,568	250,854	89,632	**982,435**
IBAC	449,463	75,524	29,504	50,173	**604,664**
ICAC (NSW)	228,803	-	-	94,256	**323,059**
ICAC (SA)	75,024	-	-	84,034	**159,058**
LECC	756,332	3,562	3,474	65,116	**828,484**
NSW CC	1,478,809	-	-	662,388	**2,141,197**
NSW Police	6,229,953	98,636	2,492,366	2,050,525	**10,871,480**
NT Police	487,288	277,131	20,000	374,882	**1,159,301**
QLD Police	4,671,810	803,741	-	68,5466	**6,161,017**
SA Police	2,131,371	234,788	3,458,858	738,372	**3,450,389**
TAS Police	623,504	5,033	10,000	170,476	**809,013**
VIC Police	858,817	18,270	208,000	134,780	**1,219,867**
WA Police	2,864,428	566,772	-	99,136	**3,530,336**
TOTAL	**39,042,417**	**2,574,995**	**12,259,422**	**7,648,407**	**58,412,241**

Emergency service facilities

Table 22 sets out the number of places that have been declared under the TIA Act to be emergency service facilities. Under the TIA Act, listening to or recording calls to and from a facility declared by the Minister to be an emergency service facility is not interception. This exemption ensures that emergency services can assist emergency callers and respond to critical situations as quickly as possible, without the need to first obtain a caller's consent to the recording of the call.

Table 22: Emergency service facility declarations

Agency	Police	Fire brigade	Ambulance	Emergency services authority	Despatching
Australian Capital Territory	5	-	-	-	3
New South Wales	8	94	6	-	6
Northern Territory	2	-	1	1	4
Queensland	21	12	9	-	13
South Australia	1	2	1	-	3
Tasmania	1	2	1	-	2
Victoria	6	1	10	-	8
Western Australia	1	2	1	-	6
TOTAL	**45**	**113**	**29**	**1**	**45**

Safeguards and reporting requirements on interception powers

The TIA Act contains a number of safeguards, controls, and reporting requirements in relation to interception, access to stored communications and disclosure of telecommunications data. These include a requirement for:

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

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

At least twice a year the Commonwealth Ombudsman must inspect the records kept by the ACIC, the ACLEI, and the AFP relating to interceptions and the use, dissemination and destruction of intercepted information. The inspections are retrospective, and for this reason, the Ombudsman inspected relevant telecommunications interception warrants that were expired or revoked in the period between 1 January and 31 December 2017.

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

While the Commonwealth Ombudsman is responsible for inspecting the records of the ACIC, the ACLEI, and the AFP in relation to interception, the relevant state or territory Ombudsman generally undertakes this function for state and territory agencies. The reports of the inspections of the declared state and territory agencies are given to the responsible state or territory minister who provides a copy to the Commonwealth Minister. The Commonwealth Ombudsman also conducts inspections of records in relation to access by enforcement agencies (including both Commonwealth and state agencies) to stored communications and telecommunications data. The Data Retention Act introduced additional obligations for these reports to be provided to the Minister and tabled in Parliament.

Commonwealth Ombudsman – inspection of telecommunications interception records

During the reporting period the Commonwealth Ombudsman conducted six inspections of the interception records of the ACIC, the ACLEI, and the AFP (two inspections for each agency) – refer to Table 23.

During its review of warrants that expired or were revoked in the period between 1 January and 31 December 2017 the Ombudsman noted there continues to be a high level of compliance with the TIA Act, where agencies displayed a good understanding of the TIA Act's requirements. The Ombudsman acknowledged agencies cooperation with, and continued disclosure of compliance issues.

Overall, the Ombudsman did not identify any systemic issues or significant problems, with all agencies found to be compliant with the majority of the Ombudsman's inspection criteria. The Ombudsman's inspection criteria (see Figures 4 and 5) are:

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

Commonwealth Ombudsman's summary of findings

Table 23: Summary of findings from the two inspections conducted at each agency between 1 January and 31 December 2017

Criteria	ACIC	ACLEI	AFP
Were restricted records properly destroyed (s 79)?	Not assessed. ACIC advised it did not conduct any destruction of restricted records during the inspection period.	Not assessed. ACLEI advised it did not conduct any destruction of restricted records during the inspection period.	Compliant
Were the requisite documents kept in connection with the issue of warrants (s 80)?	Compliant	Compliant	Compliant
Were warrant applications properly made and warrants in the correct form (ss 39(1) and 49)?	Compliant. The ACIC disclosed a non-compliance which was administrative in nature.	Compliant. Minor administrative errors in three instances.	Compliant. The AFP disclosed three non-compliances which were administrative in nature.
Were the requisite records kept in connection with interceptions (s 81)?	Compliant	Compliant with two exceptions. ACLEI disclosed two instances in which the agency had not kept records of the use and communication of lawfully intercepted information. ACLEI subsequently prepared the records after which the Ombudsman was satisfied they met the requirements of the Act.	Compliant
Were interceptions conducted in accordance with the warrants (s 7) and was any unlawfully intercepted information properly dealt with (s 63)?	Compliant. Three instances where the ACIC received information from the carrier after the warrant was revoked that was not quarantined. Upon receiving advice of the existence of this data the ACIC quickly responded by quarantining it.	Compliant	Compliant. One instance where the Ombudsman was unable to determine compliance. The Ombudsman notes there was nothing to indicate otherwise that the interception was not conducted lawfully.

Commonwealth Ombudsman's findings per Commonwealth agency for warrants expiring between 1 January to 31 December 2017

ACIC

No formal recommendations were made as a result of either of the two inspections of the ACIC.

However the Ombudsman identified three instances where intercepted information was received by the ACIC after the warrant was revoked but was not quarantined. The ACIC upon being notified of the existence of this data quickly responded by quarantining it.

The Ombudsman noted that despite this, in their view the ACIC has sufficient procedures in place to ensure that the interception of telecommunications is conducted in accordance with the Act.

ACLEI

No formal recommendations were made as a result of either of the two inspections of the ACLEI.

However, the Ombudsman identified two instances in which the ACLEI had not kept records of the use and communication of lawfully intercepted information. At the inspection, ACLEI disclosed the records had not yet been created and subsequently prepared the records and presented them to the Ombudsman. Following inspection, the Ombudsman was satisfied they met the requirements of the Act.

The Ombudsman also identified three warrants that contained minor administrative errors. These errors did not result in non-compliance as the Ombudsman was satisfied that the warrants nonetheless captured the required information. Following the inspection, ACLEI advised the Ombudsman that the relevant operational staff had been informed of the findings and were reminded of the need for appropriate attention to be paid to the preparation of documents so as to avoid the occurrence of administrative errors.

AFP

No formal recommendations were made as a result of either of the two inspections of the AFP.

However, the Ombudsman found in one instance they were unable to confirm if internet data was intercepted in accordance with the warrant. This resulted from technical limitations that precluded the internet service provider (ISP) from providing information that established a link between the intercepted IP address and the service listed on the warrant.

In turn, the Ombudsman was unable to determine whether all interceptions were conducted in accordance with the warrant, although no information was identified to indicate otherwise. The Ombudsman noted the AFP took steps to confirm the link with the ISP and acknowledge other intercepting agencies relying on this ISP would experience similar difficulties.

The Ombudsman are of the view the AFP has sufficient procedures in place to ensure that the interception of telecommunications are conducted in accordance with the Act. This was evident in two instances where the AFP responded appropriately when it identified unauthorised intercepted information.

The AFP also disclosed a number of administrative errors that resulted in non-compliance. The Ombudsman noted the actions taken by the AFP in response, outlined below:

- At the first inspection, the AFP disclosed that a warrant was issued for longer than 90 days, contrary to section 49(3) of the Act. The AFP identified the error, revoked the warrant and obtained a new warrant. At the inspection, the Ombudsman confirmed the original warrant was not executed and no information was intercepted.
- The AFP also disclosed one instance where the warrant was incorrectly dated, contrary to subsection 49(1) of the Act. The AFP identified the error and returned the warrant to the issuing authority for amendment.
- At the second inspection, the AFP disclosed one instance in which a telecommunications service warrant listed two service numbers, contrary to sections 46 and 49 of the Act. The AFP advised this occurred due to an administrative error and the warrant was revoked prior to the carrier being notified. As a result, no information was intercepted.

Figure 3: Commonwealth Ombudsman's Telecommunications Interception Inspection Criteria

Objective: to assess agencies' compliance with the record keeping and destruction requirements of the telecommunications interception provisions of the *Telecommunications (Interception and Access) Act 1979*

s 79: Destruction of restricted records

1.1: Evidence that the chief officer was satisfied that the destroyed restricted records were not likely to be required for a permitted purpose and were subsequently destroyed forthwith (s 79(1)).

1.2: Evidence that the destroyed restricted records were not destroyed before the Minister for Home Affairs had inspected the warrants under which the restricted records were obtained (s 79(2)).

s 80: Documents kept in connection with the issue of warrants

2.1: Evidence that all warrants issued to the agency are kept (s 80(a)).

2.2: Evidence that a copy of each notification under s 59A(2) is kept (notifications to the Secretary of Home Affairs) (s 80(b)).

2.3: Evidence that all instruments revoking warrants are kept (s 80(c)).

2.4: Evidence that a copy of each certificate issued under s 61(4) is kept (*evidentiary certificates*) (s 80(d)).

2.5: Evidence that each authorisation by the chief officer under s 66(2) is kept (*authorisation to receive information under warrants*) (s 80(e)).

s 81: Other records kept in connection with interceptions (Warrant details, lawfully intercepted information (LII) records, use and communication)

3.1: Evidence that each telephone application for a part 2-5 warrant is kept (s 81(1)(a)).

3.2: Evidence that statements as to whether applications were withdrawn, refused, or issued on the application are kept. (s 81(1)(a)).

3.3: Evidence that the particulars of all warrants whose authority is exercised by the agency are kept (s 81)(1)(c)(i).

3.4: Evidence that particulars of the day and time at which each interception under the warrant began (for named person warrants the service must also be indicated) are kept (ss 81(1)(c)(ii) and 81(2)).

3.5: Evidence that particulars of the duration of each interception and the name of the person who carried out each interception are kept (ss 81(1)(c)(iii) and (iv).

3.6: Evidence that particulars of each named person warrant including each service to or from which communications have been intercepted under the warrants are kept (s 81(1)(c)(v)).

3.7: Evidence that each warrant issued to the agency is kept that relates to restricted records that have at any time been in the agency's possession (s 81(1)(d)(i)).

3.8: Evidence that particulars of each occasion when the restricted record came to be in the agency's possession are kept (s 81(1)(d)(ii).

3.9: Evidence that particulars of each occasion when the restricted record ceased to be in the agency's possession are kept (s 81(1)(d)(iii).

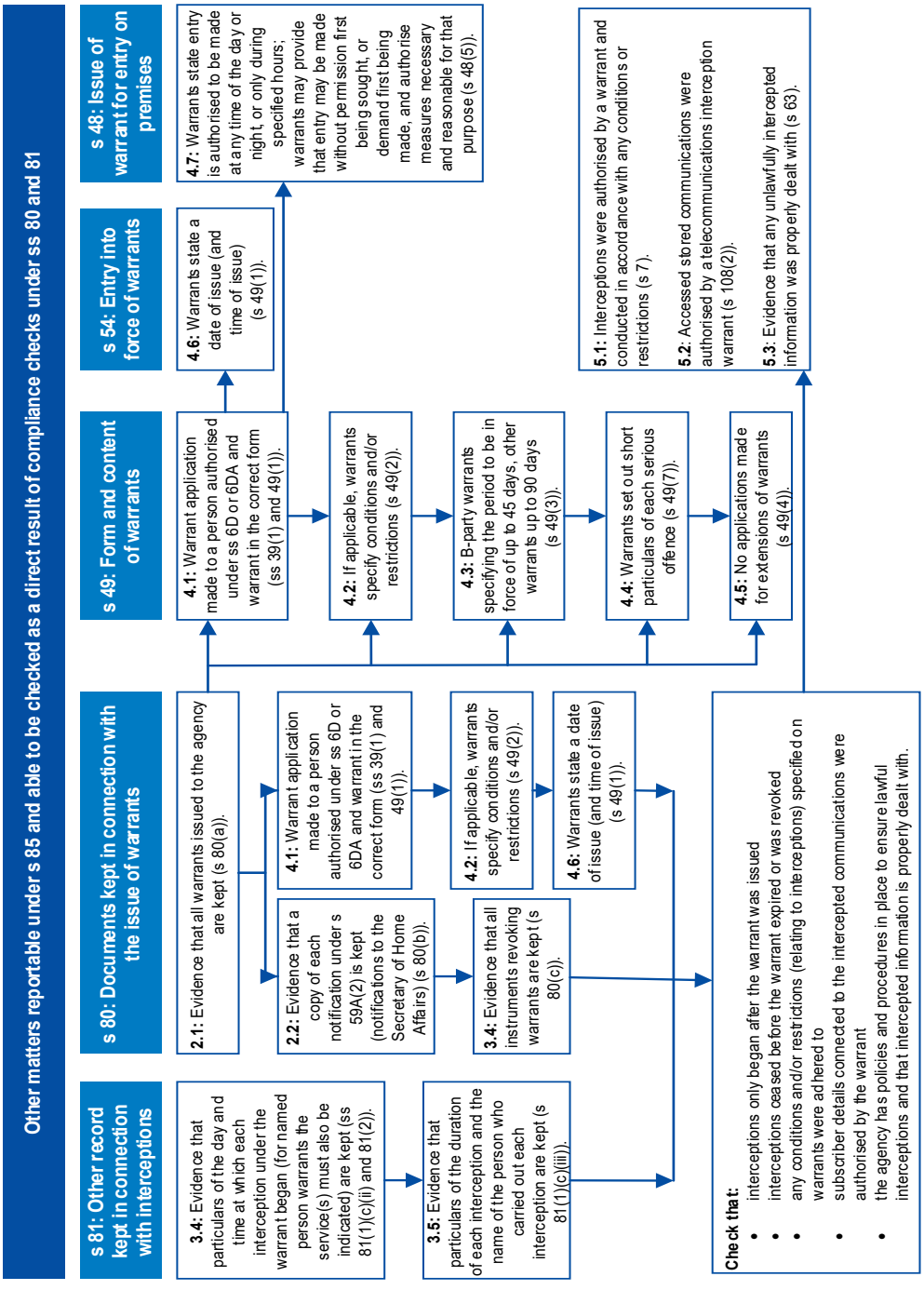
3.10: Evidence that particulars of each other agency from or to which or other person from or to whom the agency received or supplied the restricted record are kept (s 81(1)(d)(iv).

3.11: Evidence that particulars of each use made by the agency of LII are kept (s 81(1)(e)).

3.12: Evidence that particulars of each communication of LII by an officer of the agency to a person or body other than such an officer are kept (s 81(1)(f)).

3.13: Evidence that particulars of when LII was given in evidence in a relevant proceeding in relation to the agency are kept (s 81(1)(g)).

Figure 4: Other Matters reportable under section 85



CHAPTER 2 – STORED COMMUNICATIONS

Authorities and bodies that are 'criminal law enforcement agencies' under the TIA Act can apply to an independent issuing authority for a stored communications warrant to investigate a 'serious contravention' as defined in the TIA Act.

Definition

All **'criminal law enforcement agencies'** are set out in section 110A of the TIA Act. These agencies include all interception agencies as well as the Department of Home Affairs, the Australian Securities and Investments Commission and the Australia Competition and Consumer Commission.

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

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 3 years
- offences punishable by a fine of at least 210 penalty units (currently $37,800) for individuals or 900 penalty units (currently $189,000) for non-individuals such as corporations.

In 2017–18, 828 stored communications warrants were issued representing an increase on the 674 warrants issued in the 2016–17 period.

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

Agency	Relevant statistics	Applications for stored communications warrants		Telephone applications for stored communications warrants	
		16 / 17	17 / 18	16 / 17	17 / 18
ACIC	Made	3	5	-	-
ACLEI	Made	-	4	-	-
AFP	Made	50	61	-	-
ASIC	Made	-	2	-	-
CCC (QLD)	Made	13	6	-	-
CCC (WA)	Made	2	-	-	-
Home Affairs	Made	13	15	-	-
IBAC	Made	2	1	-	-
ICAC (SA)	Made	3	2	-	-
LECC	Made	1	1	-	-
NSW CC	Made	2	4	-	-
NSW Police	Made	335	405	2	4
NT Police	Made	5	2	2	-
QLD Police	Made	92	147	-	-
SA Police	Made	12	14	-	-
TAS Police	Made	49	43	-	-
VIC Police	Made	58	90	-	-
WA Police	Made	34	26	-	-
TOTAL	**Made**	**674**	**828**	**4**	**4**
	Refused	**-**	**-**	**-**	**-**
	Issued	**674**	**828**	**4**	**4**

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

Agency	16 / 17	17 / 18
CCC (QLD)	-	3
NSW Police	335	405
SA Police	12	14
TOTAL	**347**	**422**

Effectiveness of stored communications warrants

In 2017–18, criminal law enforcement agencies made 412 arrests, conducted 611 proceedings and obtained 356 convictions based on evidence obtained under stored communications warrants.

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

Agency	Arrests		Proceedings		Convictions	
	16 / 17	17 / 18	16 / 17	17 / 18	16 / 17	17 / 18
ACIC	-	1	-	-	-	-
ACLEI	-	1	-	1	-	2
AFP	14	20	-	-	-	14
CCC (QLD)	-	-	-	-	-	-
Home Affairs	-	1	-	1	-	1
IBAC	-	-	-	1	-	1
ICAC (SA)	3	-	-	-	-	-
NSW CC	-	4	-	3	-	3
NSW Police	269	215	940	430	320	164
NT Police	5	-	2	-	2	-
QLD Police	48	107	78	163	78	160
SA Police	3	11	7	4	8	1
TAS Police	-	3	-	-	-	3
VIC Police	38	49	26	8	29	7
WA Police	14	-	-	-	3	-
TOTAL	**394**	**412**	**1,053**	**611**	**440**	**356**

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 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 on the day of the notice for up to 90 days.
- *Ongoing domestic preservation notices* – requires the preservation of all communications held by the carrier for a period of 29 days from the day after the notice is received. The notice remains in force for up to 90 days."
- *Foreign preservation notices* – requires the preservation of all stored communications that a carrier holds that relate to the specified person connected with the contravention of foreign laws.

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 have been made, or a request made has been refused.

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

Agency	Domestic preservation notice	Domestic preservation revocation notices issued
ACIC	26	7
ACLEI	3	-
AFP	149	67
ASIC	94	-
CCC (QLD)	26	7
Home Affairs	18	2
IBAC	1	-
ICAC (NSW)	2	-
ICAC (SA)	10	2
LECC	9	7
NSW CC	6	1
NSW Police	558	113
NT Police	36	30
QLD Police	306	71
SA Police	88	57
TAS Police	93	51
VIC Police	141	31
WA Police	79	49
TOTAL	**1,645**	**495**

Under subsection 161A(2) of the TIA Act, the AFP is required to report on foreign preservation notices. In 2017–18, the AFP reported that eight foreign preservation notices were issued with five revocations.

Mutual assistance

Paragraph 162(1)(c) requires the report to outline the number of stored communications warrants obtained to assist in mutual assistance applications. The AFP applied for, and were issued, 10 stored communications warrants on behalf of other countries.

Paragraph 162(1)(d) requires the report must list, for each offence against a law of a foreign country in respect of which a stored communications warrant was issued as a result of a mutual 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 foreign offence. The AFP advised that the offences related to:

- an offence against Part 5.1, Division 80 of the *Criminal Code Act 1995* (Treason, urging violence and advocating terrorism or genocide)
- an offence against Part 5.2, Division 91 of the *Criminal Code Act 1995* (Espionage)
- an offence against Part 10.2 of the *Criminal Code Act 1995* (Money Laundering)
- an offence against section 11.5 of the *Criminal Code Act 1995* (Conspiracy)
- an offence against section 101.1 of the *Criminal Code Act 1995* (Terrorism)
- an offence against section 102.3 of the *Criminal Code Act 1995* (Member of a Terrorist Organisation)
- an offence against section 474.14 of the *Criminal Code Act 1995 (*Using a telecommunications service with intention to commit a serious offence).
- an offence against section 474.17 of the *Criminal Code Act 1995* (Using a carriage service to menace, harass, or cause offence).
- an offence against section 477.1 of the *Criminal Code Act 1995* (Unauthorised access, modification or impairment with intent to commit a serious offence)
- an offence against section 477.2 of the *Criminal Code Act 1995* (Unauthorised modification of data to cause impairment)
- an offence against section 477.3 of the *Criminal Code Act 1995 (*Unauthorised impairment of electronic communication)

Section 163A of the TIA Act provided that the annual report must provide information regarding the number of occasions in which lawfully accessed information or stored communications warrant information was provided to a foreign country under the Mutual Assistance Act. In 2017–18 there were two occasions on which this information was provided to a foreign country under the Mutual Assistance Act.

Ombudsman inspection report

The Commonwealth Ombudsman inspects the preservation notices and stored communications access record of all criminal law enforcement agencies. Summaries of these inspections have been included in previous annual reports.

Due to changes made through the Data Retention Act, the annual report no longer includes information on inspections concerning stored communications and preservation notices. Under section 186J the Commonwealth Ombudsman continues to have a statutory obligation to report on the results of these inspections to the Minister.

However, the Minister must now cause a copy of this report to be tabled before each House of Parliament within 15 sitting days after the receipt of the inspection report.

This requirement will ensure the Parliament and public have visibility of the inspection results outside of the annual report.

CHAPTER 3 – TELECOMMUNICATIONS DATA

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

Definition

The definition of **'enforcement agency'** is restricted to 20 agencies that also fall under the definition of 'criminal law enforcement agency'. All criminal law enforcement agencies are set out in section 110A of the TIA Act. These agencies include all interception agencies as well as the Department of Home Affairs, the Australian Securities and Investments Commission, and the Australian Competition and Consumer Commission.

During the reporting period, 20 enforcement agencies made historical data authorisations.

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.

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.

Under the TIA Act, all enforcement agencies can access historical data and criminal law enforcement agencies can also access prospective data. Disclosure of telecommunications data must be approved by an authorised senior officer of the relevant enforcement agency.

Definition

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

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

Only *criminal law enforcement agencies* can authorise the disclosure of prospective data.

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

Existing data – enforcement of a criminal law

Table 28 provides information on the use of historical data authorisations to enforce the criminal law.

Table 28: Number of authorisations made by a criminal law enforcement agency for access to existing information or documents in the enforcement of a criminal law – paragraph 186(1)(a)

Agency	Authorisations	
	16 / 17	17 / 18
ACCC	53	40
ACIC	8,177	7,498
ACLEI	629	413
AFP	22,127	19,432
ASIC	1,677	1,869
CCC (QLD)	2,993	1,271
CCC (WA)	171	123
Home Affairs	3,337	3,598
IBAC	277	701
ICAC (NSW)	207	291
ICAC (SA)	306	288
LECC	339	376
NSW CC	2,322	2,893
NSW Police	104,176	99,222
NT Police	2,308	2,105
QLD Police	22,189	25,014
SA Police	6,060	10,641
TAS Police	9,162	8,554
VIC Police	82,041	90,112
WA Police	24,518	21,338
TOTAL	**293,069**	**295,779**

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

Table 29 provides information on the use of historical data authorisations to enforce a law imposing a pecuniary penalty or protecting public revenue.

Table 29: 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)

Agency	Authorisations	
	16 / 17	17 / 18
ACCC	10	21
AFP	38	26
ASIC	101	105
Home Affairs	32	41
NSW Police	1,284	1,235
NT Police	2	1
QLD Police	4	2
SA Police	4	4
TAS Police	1,124	678
WA Police	8	-
TOTAL	**2,607**	**2,113**

Existing data – assist in locating a missing person

Table 30 provides information on the use of historical data authorisations for the location of a missing person.

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

Agency	Authorisations	
	16 / 17	17 / 18
AFP	91	178
NSW Police	1,197	1,015
NT Police	19	15
QLD Police	578	289
SA Police	63	160
TAS Police	1,092	114
VIC Police	1,256	1,345
WA Police	252	105
TOTAL	**4,548**	**3,221**

Prospective data – authorisations

Tables 31 and 32 set out information about the use of prospective data authorisations during the reporting year. The number of authorisations made by a criminal law enforcement agency for access to specified information or documents that come into existence during the period for which an authorisation is in force is contained in Table 31. The table also outlines the number of days the authorisations were to be in force and how many days they were actually in force.

Table 31: Prospective data authorisations – paragraph 186(1)(c)

Agency	Number of authorisations made	Days specified in force	Actual days in force	Authorisations discounted
ACIC	1,401	41,809	30,475	28
ACLEI	182	8,056	7,068	24
AFP	3,701	144,571	124,850	416
ASIC	17	34	33	-
CCC (QLD)	203	8,753	7,303	35
CCC (WA)	89	3,828	3,394	3
Home Affairs	264	614	604	-
IBAC	287	11,733	8,015	54
ICAC (NSW)	25	1,125	823	5
ICAC (SA)	31	1,318	1,157	31
LECC	64	2,825	2,466	-
NSW CC	1,149	48,976	45,496	110
NSW Police	1,043	19,307	15,671	48
NT Police	400	15,594	11,588	24
QLD Police	3,430	146,478	100,823	394
SA Police	342	9,407	7,985	24
TAS Police	172	7,740	4,810	11
VIC Police	9,619	384,341	329,420	1,010
WA Police	1,528	54,928	38,533	130
TOTAL	**23,947**	**911,437**	**740,514**	**2,347**

Table 32 compares information about the average number of days the authorisations were specified to be in force and the average actual number of days they remained in force between 2016–17 and 2017–18.

Table 32: Average specified and actual time in force of prospective data authorisations

Agency	Average period specified		Average period actual	
	16 / 17	17 / 18	16 / 17	17 / 18
ACIC	28	30	20	22
ACLEI	43	44	38	45
AFP	38	39	24	38
ASIC	-	2	-	2
CCC (QLD)	26	43	21	43
CCC (WA)	43	43	33	39
Home Affairs	2	2	2	2
IBAC	39	41	33	34
ICAC (NSW)	45	45	32	41
ICAC (SA)	44	43	29	37
LECC	42	44	38	39
NSW CC	42	43	37	44
NSW Police	23	19	17	16
NT Police	32	39	25	31
QLD Police	43	43	35	33
SA Police	35	28	27	25
TAS Police	45	45	25	30
VIC Police	19	40	18	38
WA Police	41	36	30	28
AVERAGE	**35**	**35**	**27**	**31**

Data authorisations for foreign law enforcement

The TIA Act also requires the AFP to report on data authorisations made in relation to foreign law enforcement. In 2017–18, the AFP made 57 data authorisations for access to telecommunications data for the enforcement of the criminal law of a foreign country.

Following these requests, the AFP made nine disclosures to foreign law enforcement agencies. Information was disclosed to the following countries: Austria, Greece (two disclosures), India, Ireland, New Zealand, the United Kingdom and the United States of America (two disclosures).

Further reporting requirements

Tables 33 and 34 set out the offences for which authorised offices of an agency made authorisations for the enforcement of the criminal law, a law imposing a pecuniary penalty, or the protection of the public revenue. 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 33: Offences for which authorisations were made to access existing data to enforce the criminal law – paragraph 186(1)(e)[8]

Categories of offences	ACCC	ACIC	ACLEI	AFP	ASIC	CCC (QLD)	CCC (WA)	Home Affairs	IBAC	ICAC (NSW)	ICAC (SA)	LECC	NSW CC	NSW Police	NT Police	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Abduction	-	-	-	456	-	-	-	-	19	-	-	-	-	7,080	151	1,841	586	561	4,015	2,169	**16,878**
ACIC Investigation	-	7,454	-	201	-	-	-	-	-	-	-	-	-	-	-	186	-	-	-	-	**7,841**
Acts - injury	-	-	-	16	-	-	-	-	20	-	-	2	-	5,123	20	14	96	342	7,508	731	**13,872**
Bribery or corruption	-	-	413	110	-	430	112	-	344	33	275	156	-	-	2	4	284	-	238	326	**2727**
Cartel offences	40	-	-	10	-	-	-	-	-	-	-	-	-	26	-	-	-	-	-	-	**76**
Conspire	-	-	-	37	12	-	-	-	-	-	-	-	-	131	1	5	1	84	356	94	**721**
Cybercrime	-	-	-	179	154	-	11	-	-	-	-	-	-	2,855	65	591	-	156	581	470	**5,062**
Dangerous acts	-	-	-	133	-	-	-	-	-	-	-	-	-	979	57	1,002	493	8	599	253	**3,524**
Fraud	-	-	-	947	646	83	-	1,391	93	254	7	69	925	11,763	79	919	1,301	512	1,377	939	**213,05**
Homicide	-	-	-	649	-	-	-	-	-	-	-	-	726	13,304	113	1,341	1,016	481	13,549	2,082	**33,261**
Illicit drug offences		44		8,200	-	632		1,876	39			126	786	22,468	1,210	4,989	3,711	3,979	12,586	6,975	**67,621**
Loss of life	-	-	-	6	-	-	-	-	-	-	-	-	17	828	5	458	60	-	5,731	2	**7,107**
Miscellaneous	-	-	-	334	1,290	71	-	7	12	-	-	-	-	4,027	97	6,222	145	19	6,084	162	**18,470**
Justice procedures	-	-	-	327	21	39	-	-	151	4	1	23	3	698	10	-	50	148	581	336	**2,392**
Organised offences	-	-	-	476	-	-	-	-	-	-	-	-	1	1,175	3	-	3	-	3,324	210	**5,192**
Pecuniary penalty	-	-	-	43	-	-	-	-	-	-	-	-	-	777	-	-	-	16	-	-	**836**

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

Categories of offences	ACCC	ACIC	ACLEI	AFP	ASIC	CCC (QLD)	CCC (WA)	Home Affairs	IBAC	ICAC (NSW)	ICAC (SA)	LECC	NSW CC	NSW Police	NT Police	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Public revenue	-	-	-	7	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**7**
People smuggling	-	-	-	110	-	-	-	74	-	-	-	-	-	2	-	-	-	-	-	-	**186**
Weapons	-	-	-	227	-	2	-	171	-	-	-	-	-	1,623	2	52	173	7	7,562	214	**10,033**
Property damage	-	-	-	56	-	-	-	-	-	-	-	-	-	1,468	4	-	31	-	5,372	4	**6,935**
Public order offences	-	-	-	9	-	-	-	-	-	-	-	-	-	63	-	48	-	-	1	88	**209**
Robbery	-	-	-	474	-	5	-	-	23	-	-	-	11	9,380	24	1,244	483	179	4,556	1,483	**17,862**
Serious damage	-	-	-	25	-	-	-	-	-	-	-	-	1	435	47	539	171	363	1,464	148	**3,193**
Sexual assault	-	-	-	415	-	4	-	6	-	-	-	-	1	7,527	126	1,752	650	305	2,591	1,406	**14,783**
Terrorism offences	-	-	-	1,627	-	-	-	5	-	-	-	-	415	800	2	-	77	19	496	83	**3,524**
Theft	-	-	-	294	3	2	-	68	-	-	5	-	6	4,507	53	1,228	285	775	5,807	1,130	**14,163**
Traffic	-	-	-	57	-	-	-	-	-	-	-	-	-	710	7	132	21	2	-	135	**1,064**
Unlawful entry	-	-	-	-	-	-	-	-	-	-	-	-	1	1,473	24	1,340	1,234	598	5,734	1,898	**12302**
TOTAL	**40**	**7,498**	**413**	**15,425**	**2,126**	**1,268**	**123**	**3,598**	**701**	**291**	**288**	**376**	**2,893**	**99,222**	**2,102**	**23,907**	**10,871**	**8,554**	**90,112**	**21,338**	**291,146**

Table 34: Offences against which authorisations were made for access to existing information or documents in enforcement of a pecuniary penalty or protection of the public revenue for the period – paragraph 186(1)(e)

Categories of offences	ACCC	AFP	ASIC	NSW Police	NT Police	QLD Police	TAS Police	WA Police	TOTAL
Abduction	-	-	-	48	-	-	64	-	**112**
Acts - injury	-	-	-	25	-	-	81	-	**106**
Cartel offences	2	-	-	-	-	-	-	-	**2**
Conspire	-	1	-	-	-	-	-	-	**1**
Cybercrime	-	-	7	17	-	-	88	-	**112**
Dangerous acts	-	-	-	40	-	-	-	-	**40**
Fraud	4	2	93	25	-	-	11	-	**135**
Homicide	-	-	-	24	-	-	-	-	**24**
Illicit drug offences		11	-	88	-	2	2	-	**103**
Loss of life	-	-	-	15	-	-	-	-	**15**
Miscellaneous	-	-	28	48	-	-	24	-	**100**
Justice procedures	-	-	1	16	-	-	152	-	**169**
Organised offences	-	1	-	458	-	-	-	-	**459**
Pecuniary penalty	15	1	-	160	-	-	74	-	**250**
Weapons	-	-	-	4	-	-	27	-	**31**
Property damage	-	-	-	46	-	-	-	-	**46**
Robbery	-	-	-	47	-	-	-	-	**47**
Sexual assault	-	9	-	33	-	-	2	-	**44**

Categories of offences	ACCC	AFP	ASIC	NSW Police	NT Police	QLD Police	TAS Police	WA Police	TOTAL
Terrorism offences	-	-	-	7	-	-	14	-	**21**
Theft	-	1	-	55	-	-	109	-	**165**
Traffic	-	-	-	44	1	-	29	11	**85**
Unlawful entry	-	-	-	35	-	-	1	-	**36**
Total	**21**	**26**	**129**	**1,235**	**1**	**2**	**678**	**11**	**2,103**

Table 35: Offences against which authorisations were made 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 (QLD)	Home Affairs	IBAC	ICAC (NSW)	ICAC (SA)	LECC	NSW CC	NSW Police	NT Police	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Abduction	-	-	100	-	-	-	-	-	-	-	-	64	11	80	-	5	1,041	40	**1,341**
ACIC Investigation	1,368	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**1,368**
Acts - injury	-	-	6	-	-	-	2	-	-	-	-	80	1	140	-	14	312	73	**628**
Bribery or corruption	-	182	19	-	100	-	169	2	19	20	-	-	8	15	-	-	11	-	**545**
Cartel offences	-	-	24	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**24**
Conspire	-	-	4	-	-	-	-	-	12	-	-	9	-	3	-	-	40	22	**90**
Cybercrime	-	-	132	-	-	-	-	-	-	-	-	4	-	-	-	-	21	0	**157**
Dangerous acts	-	-	67	-	-	13	-	-	-	-	2	8	-	11	9	-	1,178	18	**1,306**
Fraud	-	-	138	17	9	138	23	23	-	16	587	30	6	80	-	1	88	29	**1,185**
Homicide	-	-	64	-	-	7	-	-	-	-	57	88	8	242	2	13	1,193	36	**1,710**
Illicit drug offences	17		2,219		80	74		-		28	293	362	341	2,044	2	84	1,119	790	**7,453**
Loss of life	-	-	5	-	-	-	-	-	-	-	8	27	1	3	-	-	264	-	**308**
Miscellaneous	14	-	37	2	4	-	-	-	-	-	-	59	3	47	-	3	473	2	**644**
Justice procedures	-	-	123	-	9	-	93	-	-	-	1	5	8	-	23	4	15	14	**295**
Organised offences	-	-	386	-	-	-	-	-	-	-	-	8	-	7	-	-	425	-	**826**
Pecuniary penalty	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**1**
Public revenue	-	-	2	-	-	2	-	-	-	-	-	4	-	-	-	-	-	-	**8**

Categories of offences	ACIC	ACLEI	AFP	ASIC	CCC (QLD)	Home Affairs	IBAC	ICAC (NSW)	ICAC (SA)	LECC	NSW CC	NSW Police	NT Police	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
People smuggling	-	-	26	-	-	6	-	-	-	-	-	-	-	-	-	-	-	-	**32**
Weapons	2	-	60	-	-	9	-	-	-	-	2	69	-	110	5	-	178	40	**475**
Property damage	-	-	10	-	-	-	-	-	-	-	-	12	-	9	-	-	59	3	**93**
Public order offences	-	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	2	-	**3**
Robbery	-	-	62	-	1	-	-	-	-	-	3	116	2	239	8	5	533	123	**1,092**
Serious damage	-	-	1	-	-	-	-	-	-	-	-	6	4	27	1	2	258	17	**316**
Sexual assault	-	-	30	-	-	-	-	-	-	-	-	18	10	47	1	1	966	13	**1,086**
Terrorism offences	-	-	109	-	-	-	-	-	-	-	196	7	-	3	-	-	216	5	**536**
Theft	-	-	35	-	-	15	-	-	-	-	-	37	9	82	-	8	633	73	**892**
Traffic	-	-	6	-	-	-	-	-	-	-	-	2	-	-	-	-	-	13	**21**
Unlawful entry	-	-	31	-	-	-	-	-	-	-	-	27	6	241	3	32	594	217	**1,151**
TOTAL	**1,401**	**182**	**3,697**	**19**	**203**	**264**	**287**	**25**	**31**	**64**	**1,149**	**1,043**	**418**	**3,430**	**54**	**172**	**9,619**	**1,528**	**23,586**

Table 36 lists the length of time for which information or documents covered by historical data authorisations had been held by a telecommunications carrier before the authorisations for that information were made. The statistics are split into successive periods of three months and include the total number of authorisations made for data held for the lengths of time specified. The information covers the mandatory retention period for telecommunications data and provides an indication of how frequently data is accessed over two years.

During the reporting period, 75 per cent of authorisations were for data 0–3 months old. 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,[9] have been recorded as '0' months old and are included in the 0–3 month field.

Subscriber information and other customer identification information constitute the majority of authorisations included in the 0–3 month bracket. This type of information is commonly used at the beginning of an investigation to identify and eliminate suspects. During the reporting period, a significant number of authorisations for identifying information related to current subscriber checks or other information without an identifiable age.

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

Table 36: Periods 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	3	6	3	1	10	9	6	6	17	**61**
ACIC	6,871	274	176	66	42	18	8	13	30	**7,498**
ACLEI	172	30	80	30	26	15	3	18	39	**413**
AFP	13,086	2,281	1,041	1,245	548	171	151	161	1,041	**19,725**
ASIC	1,579	93	87	21	7	16	12	38	45	**1,898**
CCC (QLD)	663	247	87	69	106	48	1	9	41	**1,271**
CCC (WA)	203	3	-	5	1	-	-	-	-	**212**
Home Affairs	3,000	369	201	134	83	22	28	24	42	**3,903**
IBAC	607	32	10	8	5	8	8	2	21	**701**
ICAC (NSW)	33	8	3	14	9	11	10	11	159	**258**
ICAC (SA)	104	45	51	32	6	9	14	1	25	**287**
LECC	25	24	10	11	9	-	1	-	33	**113**
NSW CC	2,089	131	60	118	109	73	107	77	129	**2,893**
NSW Police	66,961	4,795	2,045	1,049	1,214	426	254	274	1161	**78,179**
NT Police	1,910	97	45	17	15	9	7	4	17	**2,121**
QLD Police	6,851	1,865	995	643	374	215	133	126	713	**11,915**
SA Police	7,290	1,371	529	870	223	158	68	158	555	**11,222**
TAS Police	8,586	378	141	72	32	30	22	61	20	**9,342**
VIC Police	63,108	7,621	6,593	4,315	3,565	3,497	1,336	57	20	**90,112**
WA Police	15,444	1,831	1,102	778	527	326	204	178	948	**21,338**
TOTAL	**198,585**	**21,501**	**13,259**	**9,498**	**6,911**	**5,061**	**2,373**	**1,218**	**5,056**	**263,462**

Table 37 lists 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 included 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.[10]

Table 37: Types of retained data disclosed in authorisations – paragraphs 186(1)(g) and 186(1)(h)

Agency	Item 1: subscriber data	Items 2 – 6: traffic data	TOTAL
ACCC	43	18	**61**
ACIC	4,646	2,852	**7,498**
ACLEI	188	225	**413**
AFP	15,057	4,578	**19,635**
ASIC	1,574	341	**1,915**
CCC (QLD)	1,005	266	**1,271**
CCC (WA)	93	119	**212**
Home Affairs	2,729	961	**3,690**
IBAC	555	146	**701**
ICAC (NSW)	195	96	**291**
ICAC (SA)	152	136	**288**
LECC	288	88	**376**
NSW CC	1,867	1,300	**2,893**
NSW Police	70,353	32,162	**102,515**
NT Police	1,744	377	**2,121**
QLD Police	19,081	6,224	**25,305**
SA Police	8,851	1,923	**10,794**
TAS Police	8,070	1,276	**9,352**
VIC Police	45,459	44,653	**90,112**
WA Police	16,964	4,374	**21,338**
TOTAL	**198,914**	**102,115**	**300,781**

[10] Appendix E further explains the type of data include in items 1–6 of the table at 187AA(1)

Journalist information warrants

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

During the reporting period, 58 historical data authorisations were made under two JIWs issued to the AFP.

Industry estimated cost of implementing data retention

From 13 October 2015, carriers and service providers must comply with the data retention obligations in Part 5-1A of the TIA Act. Information obtained from approximately 400 carriers and service providers, collected from industry by the Australian Communications and Media Authority, shows the cost of complying with the data retention obligations for the four financial years commencing July 2014 and ending June 2018 (set out in Table 38).

Table 38 further sets out the costs recovered from criminal law enforcement agencies (CLEAs) for the purpose of complying with their data retention obligations.

Table 38: Industry Capital Costs of data retention – subsection 187P(1A)

Financial year	Data retention compliance cost (GST inclusive) (*exclusive of data retention industry grants*)	Costs recovered from CLEAs (GST inclusive)
2014-15	$11,972,288.15	$7,316,341.41
2015-16	$44,426,132.06	$9,412,132.06
2016-17	$119,793,739.83	$9,829,783.17
2017-18	$35,355,577	$12,515,681
TOTAL	**$211,547,737.04**	**$39,073,937.64**

During the reporting period, the total funding provided under the Data Retention Industry Grants Programme was $2,508,370.21 (GST inclusive). There were 27 recipients of this funding.

CHAPTER 4 – FURTHER INFORMATION

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

National Security Policy Branch

Department of Home Affairs

PO Box 25

BELCONNEN ACT 2616

(02) 6264 1111

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

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

APPENDIX A – LISTS OF TABLES AND FIGURES

APPENDIX B – INTERCEPTION AGENCIES UNDER THE TIA ACT

Commonwealth agency or state eligible authority	Date of s.34 declaration
Australian Commission for Law Enforcement Integrity	Not applicable
Australian Criminal Intelligence Commission	Not applicable
Australian Federal Police	Not applicable
Crime and Corruption Commission (Western Australia)	26 March 2004
Crime and Corruption Commission (Queensland)	7 July 2009
Independent Broad-based Anti-corruption Commission (Victoria)	18 December 2012 (Came into force 10 February 2013)
Independent Commission Against Corruption (New South Wales)	6 June 1990
New South Wales Crime Commission	30 January 1989
New South Wales Police Force	30 January 1989
Northern Territory Police	25 October 2006
Law Enforcement Conduct Commission	14 July 1998
Queensland Police Service	8 July 2009
Independent Commissioner Against Corruption (South Australia)	17 June 2013 (came into force 1 September 2013)
South Australia Police	10 July 1991
Tasmania Police	5 February 2005
Victoria Police	28 October 1988
Western Australia Police	15 July 1997

APPENDIX C – ABBREVIATIONS

Acronym	Agency/Organisation
AAT	Administrative Appeals Tribunal
ACIC	Australian Criminal Intelligence Commission
ACCC	Australian Competition and Consumer Commission
ACLEI	Australian Commission for Law Enforcement Integrity
AFP	Australian Federal Police
AGD	Attorney-General's Department
ASIC	Australian Securities and Investments Commission
CAC	Communications Access Co-ordinator
CCC (WA)	Corruption and Crime Commission (Western Australia)
CCC (QLD)	Crime and Corruption Commission (Queensland)
Home Affairs	Department of Home Affairs
IBAC	Independent Broad-based Anti-corruption Commission (Victoria)
LECC	Law Enforcement Conduct Commission
NSW CC	New South Wales Crime Commission
ICAC (NSW)	Independent Commission Against Corruption (New South Wales)
NSW Police	New South Wales Police Force
NT Police	Northern Territory Police
PIM	Public Interest Monitor
PJCIS	Parliamentary Joint Committee on Intelligence and Security
QLD Police	Queensland Police Service
ICAC (SA)	Independent Commissioner Against Corruption (South Australia)
SA Police	South Australia Police
TAS Police	Tasmania Police
Telecommunications Act	Telecommunications Act 1997
TIA Act	Telecommunications (Interception and Access) Act 1979
VIC Police	Victoria Police
WA Police	Western Australia Police

APPENDIX D – CATEGORIES OF SERIOUS OFFENCES

Serious offence category	Offences covered
ACIC special investigation	TIA Act, s5D(1)(f)
Administration of justice	TIA Act, s5D(8)(b): offences against ss35, 36, 36A, 37, 39, 41, 42, 43, 46 or 47 of the Crimes Act 1914
Assist escape punishment/dispose of proceeds	TIA Act, s5D(7)
Bribery or corruption; offences against ss131.1, 135.1, 142.1, 142.2, 148.2, 268.112 of the Criminal Code	TIA Act, s5D(2)(vii); TIA Act, s5D(8)(a): offences against ss131.1, 135.1, 142.1, 142.2, 148.2 or 268.112 of the Criminal Code Act 1995
Cartel offences	TIA Act, s5D(5B)
Child pornography offences	TIA Act, s5D(3B)
Conspire/aid/abet serious offence	TIA Act, s5D(6)
Cybercrime offences	TIA Act, s5D(5)
Espionage and foreign interference offences	TIA Act, s5D(1)(e)(ic),(id),(ie),(if) and (ig)
Kidnapping	TIA Act, s5D(1)(b)
Loss of life or personal injury	TIA Act, s5D(2)(b)(i) and (ii)
Money laundering	TIA Act, s5D(4)
Murder	TIA Act, s5D(1)(a)
Organised offences and/or criminal organisations	TIA Act, s5D(3; s5D(8A) and (9)
People smuggling and related	TIA Act, s5D(3A)
Serious damage to property and/or serious arson	TIA Act, s5D(2)(b)(iii) and (iiia)
Serious drug offences and/or trafficking	TIA Act, s5D(5A); s5D(2)(b)(iv); TIA Act, s5D(1)(c)
Serious fraud and/or revenue loss	TIA Act, s5D(2)(v) and (vi)
Telecommunications offences	TIA Act, s5D(5)(a)
Terrorism offences	TIA Act, s5D(1)(d), 5D(1)(e)

APPENDIX E – RETAINED DATA SETS

Item	Description of information	Explanation
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; i. 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 more of the following i. billing or payment information; i. contract 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 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
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. • 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
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.
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 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
The type of a 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 enabled 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 (5(b)) 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).
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 Act provides that location records are limited to information that is used by a service provider in relation to the relevant service. This would include information such as which cell tower, Wi-Fi hotspot or base station a device was connected to at the start and end of communication. Service providers are not required to keep continuous, real-time, or precise location records, such as the continuous GPS location of a device. These limitations seek to ensure that the location records to be kept by service providers do not allow continuous monitoring or tracking of devices.

APPENDIX F – CATEGORIES OF OFFENCES ABBREVIATIONS

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

NOTES

www.homeaffairs.gov.au