Australian Government
Department of Home Affairs

TELECOMMUNICATIONS (INTERCEPTION AND ACCESS) ACT 1979

Annual Report 2016–17

www.homeaffairs.gov.au

ISBN: 978-1-920838-32-4 (Print)

ISBN: 978-1-920838-33-1 (Online)

Contact us

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

Department of Home Affairs
PO Box 25
BELCONNEN ACT 2616

www.homeaffairs.gov.au

TELECOMMUNICATIONS (INTERCEPTION AND ACCESS) ACT 1979

Annual Report 2016–17

CONTENTS

EXECUTIVE SUMMARY

The *Telecommunications (Interception and Access) Act 1979 Annual Report 2016–17* 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* (TIA Act) between 1 July 2016 — 30 June 2017.

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 and persons 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 to intercept and access stored communications is independently overseen by the Commonwealth Ombudsman and equivalent state bodies.

Legislative reforms

Counter-Terrorism Legislation Amendment Act (No. 1) 2016

The *Counter-Terrorism Legislation Amendment Act (No. 1) 2016* amended the TIA Act to establish a regime for monitoring the compliance of individuals who are the subject of a control order through telecommunications interception warrants. The regime includes essential safeguards such as a threshold for issuing warrants, ministerial and reporting requirements, and independent oversight by the Commonwealth Ombudsman.

Law Enforcement Legislation Amendment (State Bodies and Other Measures) Act 2016

The *Law Enforcement Legislation Amendment (State Bodies and Other Measures) Act 2016* (LELA) replaced references to the NSW Police Integrity Commission (PIC) with the Law Enforcement Conduct Commission (LECC). The LECC is responsible for the detection, investigation and prevention of law enforcement corruption and misconduct.

The LELA amended the TIA Act to include the LECC within the definition of 'eligible authority'. This allows the Attorney-General to declare the LECC an 'interception agency'[1] and include it within the definition of a criminal law enforcement agency for the purposes of section 110A of the TIA Act.

1 If requirements under section 35 of the TIA Act are satisfied by the respective State legislation.

Key judicial decisions

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

Key findings

- In 2016–17, 3,717 interception warrants were issued.
- During 2016–17, information obtained under interception warrants was used in:[2]
  - 3,369 arrests[3]
  - 4,318 prosecutions
  - 2,703 convictions.
- In 2016–17, 20 enforcement agencies made 300,224 authorisations for the disclosure of historical telecommunications data. Of these, 293,069 authorisations were made to enforce a criminal law.
  - This represents a decrease from 2015-2016. In 2015-2016, 63 enforcement agencies made 333,980 authorisations for the disclosure of historical telecommunications data. Of those, 326,373 authorisations were made to enforce a criminal law.
- During 2016–17, the majority of criminal law offences for which historical data was requested were illicit drug offences (71,684 requests). 33,358 requests were made for homicide and related offences and 18,856 requests were made for fraud.
- In 2016–17, law enforcement agencies made 394 arrests, conducted 1,064 proceedings and obtained 442 convictions based on evidence obtained under stored communications warrants.[4]

Access to the content of a communication

Accessing content, or the substance of a communication—for instance, the message written in an email, the discussion between two parties to a phone call, the subject line of an email or a private social media post—without the knowledge of the person making the communication is highly intrusive. Under the TIA Act, unless access occurs in certain limited circumstances, such as a life threatening emergency, 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.

2 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.

3 This figure includes the number of times lawfully intercepted information culminated in an arrest.

4 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.

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.[5]

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 2016–17 reporting period all enforcement agencies could access historical data[6] and only criminal law enforcement agencies could access prospective data to assist in the investigation of offences punishable by at least three years' imprisonment.[7] 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 telecommunications data to 20 specified agencies. The Minister may declare additional agencies in prescribed circumstances. No additional agencies were prescribed in the 2016–17 reporting period.

5 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.

6 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.

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

Format of Annual Report

This Annual Report is organised into three main chapters:

- Chapter 1—telecommunications interception,
- Chapter 2—stored communications
- 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 Australian Federal Police 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 warrants 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 AFP
- state and territory police
- 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.[8]

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 2016–17 the majority of warrants obtained were to assist with investigations into serious drug offences (1,953 warrants). Loss of life or personal injury offences were specified in 587 warrants and 258 warrants related to murder investigations. Money laundering was specified as an offence in 319 warrants. The total number of offences is typically larger than the total number of warrants issued, as warrants can be issued to investigate more than one serious offence.

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

8 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
ACC special investigation	225	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	225
Administration of justice	-	-	5	-	-	-	-	-	-	-	-	-	-	-	-	-	-	5
Bribery, corruption and dishonesty offences	-	17	55	32	37	8	5	17	2	-	7	3	-	-	-	12	4	199
Cartel offences	-	-	7	-	-	-	-	-	-	-	-	-	-	-	-	-	-	7
Child pornography offences	-	-	4	-	-	-	-	-	-	-	-	-	-	-	-	-	-	4
Conspire/aid/abet serious offence	-	-	2	-	-	-	-	8	-	10	15	-	-	-	6	5	-	46
Cybercrime offences	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1
Kidnapping	-	-	-	-	-	-	-	-	-	3	27	-	-	-	-	3	-	33
Loss of life or personal injury	-	-	121	-	-	-	-	-	-	16	339	-	30	4	-	48	29	587
Money laundering	15	-	251	-	-	1	-	-	-	49	2	-	-	-	-	-	1	319
Murder	-	-	3	-	-	-	-	-	-	21	154	1	9	15	13	17	25	258
Organised offences and/or criminal organisations	-	-	16	-	-	-	-	-	-	3	163	1	-	-	-	10	3	196
People smuggling and related	-	-	4	-	-	-	-	-	-	-	-	-	-	-	-	-	-	4
Serious damage to property and/or serious arson	-	-	3	-	-	-	-	-	-	-	71	-	1	1	2	5	7	90
Serious drug offences and/or trafficking	16	10	690	9	-	2	-	-	-	68	662	26	199	51	9	80	131	1,953
Serious fraud	-	-	25	2	-	2	-	-	-	8	52	-	12	2	-	9	6	118
Serious loss of revenue	-	-	38	-	-	-	-	-	-	-	-	-	-	-	-	-	-	38
Telecommunications offences	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	-	1
Terrorism financing offences	-	-	5	-	-	-	-	-	-	-	-	-	-	-	-	-	-	5
Terrorism offences	-	-	50	-	-	-	-	-	-	9	6	-	-	-	-	-	-	65
Total	**256**	**27**	**1,280**	**43**	**37**	**13**	**5**	**25**	**2**	**187**	**1,499**	**31**	**251**	**73**	**30**	**189**	**206**	**4,154**

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 2017, there were 89 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 2017—s. 103(ab)

Issuing authority	Number eligible
Federal Court judges	16
Family Court judges	6
Federal Circuit Court judges	36
Nominated AAT members	31

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
- 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 detailing which authorities issued warrants to each of the interception agencies in the reporting period. In 2016–17, issuing authorities issued 3,717 interception warrants, a decrease from 2015–16, when 3,857 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 —s. 103(ab)

Agency	Issuing authority			
	Family Court judges	Federal Circuit Court Judges	Federal Court Judges	Nominated AAT members
ACLEI	-	12	-	15
ACIC	1	18	-	223
AFP	2	42	1	858
CCC (QLD)	-	16	-	26
CCC (WA)	23	-	1	13
IBAC	-	13	-	-
ICAC (NSW)	-	-	-	5
ICAC (SA)	-	2	-	23
LECC	-	-	-	2

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

Agency	Relevant statistics	Applications for warrants		Telephone applications for warrants[8]		Renewal applications[9]	
		15/16	16/17	15/16	16/17	15/16	16/17
ACIC	Made	260	242	-	-	37	33
ACLEI	Made	6	27	-	-	2	13
AFP	Made	1,012	904	-	-	284	312
	Refused	1	1	-	-	1	-
CCC (QLD)	Made	27	44	-	-	1	17
	Refused	-	2	-	-	-	-
CCC (WA)	Made	25	37	-	-	7	7
IBAC	Made	20	13	1	-	2	4
ICAC (NSW)	Made	13	5	-	-	6	2
ICAC (SA)	Made	8	26	-	-	-	2
	Refused	-	1	-	-	-	-
LECC	Made	60	2	-	-	31	-
NSW CC	Made	165	150	-	-	45	54
NSW Police	Made	1,430	1,499	30	18	262	325
NT Police	Made	41	31	-	-	1	2
QLD Police	Made	243	251	-	-	38	37
SA Police	Made	101	65	-	-	6	3
TAS Police	Made	15	30	-	-	1	-
VIC Police	Made	150	189	14	4	9	18
WA Police	Made	282	206	-	-	33	13
TOTAL	**Made**	**3,858**	**3,721**	**45**	**22**	**765**	**842**
	Refused	**1**	**4**	**-**	**-**	**1**	**-**
	Issued	**3,857**	**3,717**	**45**	**22**	**764**	**842**

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.

Table 5: Applications for telecommunications interception warrants authorising entry on premises—ss. 100(1)(d) and 100(2)(d)

Agency	Relevant statistics	Warrants authorising entry on premises	
		15/16	16/17
AFP	Made	2	1
	Refused/withdrawn	-	-
Total	**Made**	**2**	**1**
	Refused/withdrawn	**-**	**-**

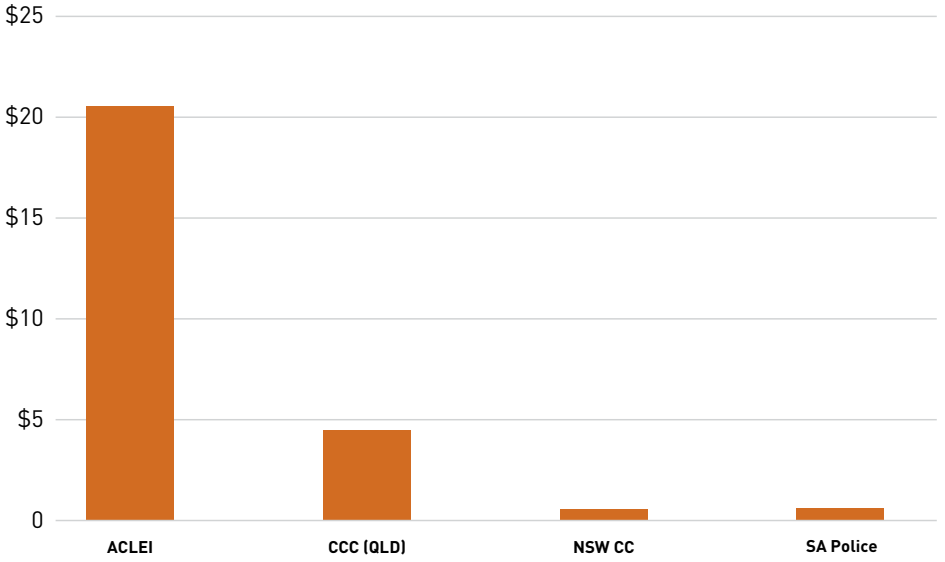
Conditions or restrictions on warrants

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, 27 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—ss. 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 not equate to the number of charges laid as an arrested person 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 the intercepted information to be admitted into evidence.

In 2016–17 there were 3,369 arrests based on lawfully intercepted information (this figure includes instances were lawfully intercepted information culminated in an arrest). There were also 4,318 prosecutions and 2,703 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—ss. 102(1)(a) and 102(2)(a)

Agency	15/16		16/17	
	Number of Arrests	Number of times lawfully intercepted information culminated in an arrest	Number of Arrests	Number of times lawfully intercepted information culminated in an arrest
ACIC	-	152	-	115
ACLEI	-	3	1	1
AFP	210	82	118	84
CCC (QLD)	48	7	33	8
CCC (WA)	-	-	-	-
IBAC	-	1	-	-
ICAC (SA)			5	5
LECC	2	1	-	-
NSW CC	-	54	-	49
NSW Police	1,291	-	1,165	-
NT Police	35	-	37	11
QLD Police	428	-	429	-
SA Police	86	3	63	-
TAS Police	5	-	21	21
VIC Police	242	2	283	66
WA Police	367	-	357	497
TOTAL	**2,714**	**305**	**2,512**	**857**

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

ACC special investigations	1	-	-	-	-	-	-	-	-	-	-	-	-	-	1
Assisting person to escape or dispose of proceeds	-	-	-	-	-	-	-	3	-	-	-	-	-	-	3
Bribery or corruption	-	2	1	10	2	2	-	-	-	-	-	-	-	3	20
Child pornography offences	-	-	1	-	-	-	-	-	-	-	-	-	-	-	1
Conspire/aid/abet serious offence	-	-	-	-	-	-	-	-	7	-	-	1	8	-	16
Kidnapping	-	-	5	-	-	-	-	-	44	-	-	-	-	-	49
Loss of life	-	-	-	-	-	-	-	-	-	-	1	-	5	-	6
Money laundering	-	-	19	-	-	-	1	30	28	-	-	-	-	-	78
Murder	-	-	-	-	-	-	-	13	61	-	6	3	4	10	97
Offences involving planning and organisation	-	-	-	-	-	-	-	-	68	-	-	-	1	511	580
Organised crime	-	-	-	-	-	-	-	-	4	-	-	-	-	-	4
Other offence punishable by 3 years to life	-	2	10	-	-	-	-	-	12	-	106	-	109	-	239
People smuggling and related	-	-	1	-	-	-	-	-	-	-	-	-	-	-	1
Serious arson	-	-	2	-	-	-	-	-	4	-	-	-	3	5	14
Serious damage to property	-	-	-	-	-	-	-	-	-	-	-	-	-	17	17
Serious drug offences	-	-	7	-	-	-	2	-	247	33	-	-	-	-	289
Serious drug offences and/or trafficking	-	-	68	-	-	-	-	-	-	-	-	-	-	-	68
Serious fraud	-	-	7	16	3	-	2	-	9	-	2	-	2	3	44
Serious personal injury	-	-	6	-	-	-	-	-	70	-	5	-	12	11	104
Telecommunications offences	-	-	-	-	-	-	-	-	21	-	-	-	-	-	21
Terrorism offences	-	-	8	-	-	-	-	-	-	-	-	-	-	-	8
Trafficking in prescribed substances	-	-	4	-	-	-	-	102	356	-	82	44	97	1,973	2,658
TOTAL	**1**	**4**	**139**	**26**	**5**	**2**	**5**	**148**	**931**	**33**	**202**	**48**	**241**	**2,533**	**4,318**

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

ACC special investigations	1	-	-	-	-	-	-	-	-	-	-	-	-	1
Assisting person to escape or dispose of proceeds	-	-	-	-	-	-	2	-	-	-	-	-	-	2
Bribery or corruption	-	2	-	-	2	-	-	-	-	-	-	-	2	6
Conspire/aid/abet serious offence	-	-	-	-	-	-	-	12	-	-	-	6	-	18
Kidnapping	-	-	2	-	-	-	-	25	-	-	-	-	-	27
Loss of life	-	-	-	-	-	-	-	-	-	1	-	4	-	5
Money laundering	-	-	2	-	-	-	18	2	-	-	-	-	-	22
Murder	-	-	-	-	-	-	10	46	-	6	3	2	6	73
Offences involving planning and organisation	-	-	-	-	-	-	-	27	-	-	-	-	355	382
Organised crime	-	-	-	-	-	-	-	2	-	-	-	-	-	2
Other offence punishable by 3 years to life	-	7	3	-	-	-	-	30	-	106	-	100	-	246
Serious arson	-	-	2	-	-	-	-	1	-	-	-	2	2	7
Serious damage to property	-	-	-	-	-	-	-	-	-	-	-	-	7	7
Serious drug offences	-	-	1	-	-	2	-	71	5	-	-	-	-	79
Serious drug offences and/or trafficking	-	-	24	-	-	-	-	-	-	-	-	-	-	24
Serious fraud	-	-	-	2	-	-	-	16	-	2	-	2	1	23
Serious personal injury	-	-	2	-	-	-	-	92	-	5	-	9	6	114
Terrorism offences	-	-	3	-	-	-	-	-	-	-	-	-	-	3
Trafficking in prescribed substances	-	-	3	-	-	-	81	137	-	81	32	92	1,236	1,662
TOTAL	**1**	**9**	**42**	**2**	**2**	**2**	**111**	**461**	**5**	**201**	**35**	**217**	**1,615**	**2,703**

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
- 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 2016–17, 824 named person warrants were issued, a decrease from the 2015–16 reporting period in which 964 named person warrants were issued.

In 2016–17, only a single named person warrant was issued with a condition or restriction, to the NSW CC.

Table 9: Original applications for named person warrants, telephone applications for named person warrants, and renewal applications—ss. 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	
		15/16	16/17	15/16	16/17	15/16	16/17
ACIC	Made	184	129	-	-	34	24
AFP	Made	388	323	-	-	157	120
	Refused/Withdrawn	-	1	-	-	-	-
CCC (QLD)	Made	3	14	-	-	-	6
CCC (WA)	Made	3	10	-	-	3	4
IBAC	Made	1	-	1	-	-	-
NSW CC	Made	70	87	-	-	22	25
NSW Police	Made	120	119	-	-	25	42
NT Police	Made	2	-	-	-	-	-
QLD Police	Made	49	42	-	-	8	5
SA Police	Made	19	5	-	-	2	-
TAS Police	Made	7	6	-	-	1	-
VIC Police	Made	46	59	3	-	5	12
WA Police	Made	72	31	-	-	9	2
TOTAL	**Made**	**964**	**825**	**4**	**-**	**266**	**240**
	Refused/Withdrawn	**-**	**1**	**-**	**-**	**-**	**-**
	Issued	**964**	**824**	**4**	**-**	**266**	**240**

Consistent with the last reporting period, in 2016–17 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—ss. 100(1)(eb) and 100(2)(eb)

Agency	Relevant statistics							
	1 service only		2 – 5 services		6 – 10 services		10+ services	
	15/16	16/17	15/16	16/17	15/16	16/17	15/16	16/17
ACIC	67	28	95	94	16	5	3	-
ACLEI	-	-	-	-	-	-	-	-
AFP	119	133	244	175	20	10	-	3
CCC (QLD)	1	4	2	10	-	-	-	-
CCC (WA)	-	-	1	7	-	1	2	1
IBAC	-	-	1	-	-	-	-	-
NSW CC	26	47	39	36	4	2	-	-
NSW Police	25	35	92	74	2	8	1	2
NT Police	-	-	2	-	-	-	-	-
QLD Police	9	16	32	22	8	2	-	-
SA Police	5	2	14	3	-	-	-	-
TAS Police	1	1	1	4	5	1	-	-
VIC Police	9	13	32	35	5	10	-	1
WA Police	16	13	54	17	2	1	-	-
Total	**278**	**292**	**609**	**477**	**62**	**40**	**6**	**7**

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

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

(i) services intercepted under service based named person warrants

(ii) services intercepted under device based named person warrants, and

(iii) telecommunications devices intercepted under device based named person warrants.

Figure 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—ss. 100(1)(ec) and 100(2)(ec)

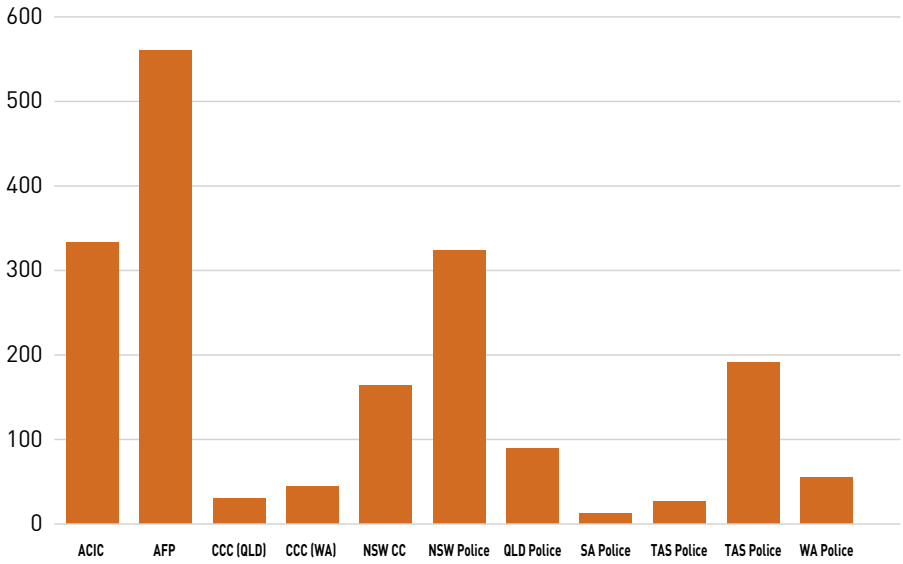


Table 11 shows that in 2016–17, device-based named person warrants were used by only a small number of agencies. This is consistent with 2015–16.

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

Agency	Devices	Services
ACIC	6	15
AFP	137	111
NSW CC	1	-
NSW Police	6	24
VIC Police	2	6
TOTAL	**152**	**156**

9 The number of services intercepted under device based warrants is unavailable for the AFP during the reporting period and will be updated in the next Annual Report.

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 interception of communications from that person's telecommunications services would not otherwise be possible.

Table 12 shows that in 2016–17, 139 B-Party warrants were issued. This represents an increase on the 108 B-Party warrants issued in 2015–16.

Table 12: Applications for B-Party warrants, telephone applications for B-Party warrants, and renewal applications—ss. 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	
		15/16	16/17	15/16	16/17	15/16	16/17
ACIC	Made	-	1	-	-	-	-
AFP	Made	60	102	-	-	26	79
	Refused	1	-	-	-	1	-
CCC (WA)	Made	-	2	-	-	-	-
NSW CC	Made	4	1	-	-	-	-
NSW Police	Made	43	29	9	3	-	2
QLD Police	Made	2	1	-	-	-	-
VIC Police	Made	-	3	-	-	-	-
TOTAL	**Made**	**109**	**139**	**9**	**3**	**26**	**81**
	Refused	**1**	**-**	**-**	**-**	**1**	**-**
	Issued	**108**	**139**	**9**	**3**	**25**	**81**

Table 13: B-Party warrants issued with conditions or restrictions—ss. 100(1)(ed) and 100(2)(ed)

Agency	Applications for B-Party warrants	
	15/16	16/17
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—ss. 101(1)(a)-(d) and 101(2)(a)-(d)

Agency	Duration of original telecommunications interception warrants		Duration of renewal of 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	51	72	89	89
ACLEI	90	75	90	85
AFP	81	62	77	81
CCC (QLD)	77	76	80	57
CCC (WA)	87	58	90	39
IBAC	90	90	82	75
ICAC (NSW)	90	58	90	78
ICAC (SA)	64	37	60	19
LECC	90	46	-	-
NSW CC	80	67	86	74
NSW Police	53	40	60	49
NT Police	86	65	90	83
QLD Police	74	55	76	65
SA Police	74	59	35	29
TAS Police	84	67	-	-
VIC Police	76	54	64	41
WA Police	88	48	90	80
AVERAGE	**79**	**61**	**77**	**63**

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—ss. 101(1)(da) and 101(2)(da)

Agency	Duration of original telecommunications B-Party warrants		Duration of renewal of telecommunications B-Party warrants	
	Average period specified in the warrant (days)	Average period the warrant was in force (days)	Average period specified in a single warrant (days)	Average period warrants were in force (days)
ACIC	45	45	-	-
AFP	45	43	44	39
CCC (WA)	45	-	-	-
NSW CC	21	21	-	-
NSW Police	32	14	41	78
QLD Police	11	11	-	-
VIC Police	45	45	-	-
AVERAGE	**35**	**30**	**43**	**59**

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
- 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—ss. 101(1)(e) and 101(2)(e)

Agency	90 days		150 days		180 days	
	15/16	16/17	15/16	16/17	15/16	16/17
ACIC	7	5	15	11	5	9
ACLEI	-	-	-	-	1	-
AFP	26	20	46	65	42	81
CCC (QLD)	-	5	-	4	-	1
CCC (WA)	2	2	3	-	1	-
IBAC	1	1	1	3	-	-
ICAC (NSW)	1	1	1	1	1	-
LECC	1	-	6	-	5	-
NSW CC	6	1	4	4	5	4
NSW Police	137	137	16	17	16	39
NT Police	1	2	-	-	-	-
QLD Police	14	9	12	11	3	4
SA Police	2	1	2	-	-	-
TAS Police	1	-	-	-	-	-
VIC Police	5	13	3	3	-	1
WA Police	4	2	12	6	6	5
TOTAL	**208**	**199**	**121**	**125**	**85**	**144**

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—ss. 102(3) and 102(4)

Agency	Total number of warrants	Number of eligible warrants	%
ACC	286	149	52
ACLEI	2	23	9
AFP	1,091	581	53
CCC (QLD)	47	43	91
CCC (WA)	37	12	32
IBAC	15	7	47
ICAC (NSW)	5	5	100
ICAC (SA)	32	7	22
LECC	7	4	57
NSW CC	190	143	75
NSW Police	1,818	1,282	72
NT Police	27	11	41
QLD Police	288	275	95
SA Police	75	50	67
TAS Police	33	20	61
VIC Police	204	126	62
WA Police	261	125	48
TOTAL	**4,418**	**2,863**	**65**

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 communication.

Table 18: Interception without a warrant—s. 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	
	15/16	16/17	15/16	16/17	15/16	16/17	15/16	16/17
NSW Police	11	4	11	-	-	-	-	-
TOTAL	**11**	**4**	**11**	**-**	**-**	**-**	**-**	**-**

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). One authorisation issued under section 13A during the reporting period included telecommunications 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—s. 103(ac)

Interception carried out by:	Interception carried out on behalf of:	Number of interceptions:
ACIC	CMC (QLD)	42
AFP	ACLEI	119
	ACIC	4
IBAC	ICAC (SA)	23
VIC Police	TAS Police	30
TOTAL		**218**

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—ss. 103(a) and 103(aa)

Police	Total expenditure ($)	Average expenditure ($)
ACIC	7,660,582	31,655
ACLEI	773,360	28,642
AFP	14,704,870	16,284
CCC (QLD)	1,726,758	41,113
CCC (WA)	1,770,830	47,860
IBAC	1,602,799	123,292
ICAC (NSW)	101,191	20,238
ICAC (SA)	222,250	8,890
LECC	1,558,860	779,430
NSW CC	2,443,644	16,290
NSW Police	9,148,034	6,609
NT Police	2,383,376	76,883
QLD Police	6,191,424	24,667
SA Police	3,982,389	61,267
TAS Police	664,898	22,163
VIC Police	7,262,943	38,428
WA Police	3,370,782	16,363
TOTAL	**65,569,230**	**-**

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	6,135,329	118,860	297,917	1,108,476	7,660,582
ACLEI	641,899	86,207	-	45,494	773,600
AFP	9,729,978	944,708	1,508,595	2,521,589	14,704,870
CCC (QLD)	1,127,646	169,060	-	430,052	1,726,758
CCC (WA)	1,037,088	3,524	654,615	75,603	1,770,830
IBAC	1,211,862	40,424	185,872	164,641	1,602,799
ICAC (NSW)	53,505	-	-	47,686	101,191
ICAC (SA)	135,504	-	-	86,746	222,250
LECC	700,868	-	819,757	38,235	1,558,860
NSW CC	1,919,630	-	-	524,014	2,443,644
NSW Police	5,747,739	117860	1,876,231	1,406,204	9,148,034
NT Police	482,375	288,692	1,300,000	312,309	2,383,376
QLD Police	4,569,430	669,038	-	952,956	6,191,424
SA Police	2,743,361	486,011	326,506	426,511	3,982,389
TAS Police	554,898	-	60,000	50,000	664,898
VIC Police	5,888,338	100,740	313,794	960,071	7,262,943
WA Police	2,901,578	340,506	-	128,698	3,370,782
TOTAL	**45,581,028**	**3,365,630**	**7,343,287**	**9,279,285**	**65,569,230**

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 recording of the call.

Table 22: Emergency service facility declarations

State/territory	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
- 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, 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 2016.

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, 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, ACLEI and the AFP (two inspections for each agency) – refer to Table 23.

During its review of warrants that expired or revoked in the period between 1 January and 31 December 2016 the Ombudsman noted that 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 noted agency responsiveness towards inspection findings.

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 3 and 4) are:

1. Were restricted records properly destroyed (s 79)?
2. Were the requisite documents kept in connection with the issue of warrants (s 80)?
3. Were warrant applications properly made and warrants in the correct form (ss 39(1) and 49)?
4. Were the requisite records kept in connection with interceptions (s 81)?
5. Were interceptions conducted in accordance with the warrants (s 7) and was any unlawfully intercepted information properly dealt with (s 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 2016

CRITERIA	ACIC	ACLEI	AFP
Were restricted records properly destroyed (s 79)?	Not assessed. The ACIC advised it did not conduct any destruction of restricted records during the inspection period.	Not assessed. The ACLEI advised it did not conduct any destruction of restricted records during the inspection period.	Compliant with the exception of twenty-four instances. Despite this the Ombudsman notes that the implemented measures to address destruction processes by the AFP are sufficient and the Ombudsman will closely monitor the effectiveness of these changes.
Were the requisite documents kept in connection with the issue of warrants (s 80)?	Compliant with the exception of one instance. Despite this the Ombudsman notes that the ACIC procedures are sufficient.	Compliant.	Compliant.
Were warrants properly applied for and in the correct form (ss 39(1) and 49)?	Compliant with the exception of one instance. The ACIC also self-disclosed three administrative errors. Despite this the Ombudsman notes that the ACIC procedures are sufficient.	Nothing to indicate otherwise.	Compliant with the exception of one instance and three instances were self-disclosed by the AFP. Despite this the Ombudsman notes that the AFP procedures are sufficient.
Were requisite records kept in connection with interceptions (s 81)?	Compliant.	Compliant.	Compliant.
Were interceptions conducted in accordance with the warrants (s 7) and was any unlawfully intercepted information properly dealt with (s 63)?	Compliant with the exception of one instance. Despite this the Ombudsman notes that the ACIC procedures are sufficient.	Compliant.	Compliant.

Commonwealth Ombudsman's findings per Commonwealth agency for warrants expiring between 1 January to 31 December 2016

ACIC

No formal recommendations were made as a result of either of the two inspections of the ACIC. However, the Ombudsman noted that the ACIC was not compliant in one instance in relation to its record keeping obligations. The Ombudsman noted that the ACIC intends to implement processes to ensure compliance with its record keeping requirements.

In response to self-disclosed instances by the ACIC regarding administrative errors, the Ombudsman noted that the ACIC had already taken action in response to the issue and that the ACIC intended to reiterate the importance of quality assurance.

ACLEI

No formal recommendations or suggestions were made as a result of either of the two inspections of ACLEI. The Ombudsman noted that ACLEI was cooperative and forthcoming with information at the inspection.

AFP

No formal recommendations were made as a result of either of the two inspections of the AFP. However the Ombudsman noted that the AFP was not compliant in relation to twenty-four instances in relation to its destruction obligations. The Ombudsman noted that the AFP has implemented a number of measures to address this issue and the Ombudsman will continue to monitor this at future inspections.

The Ombudsman noted two instances where the AFP self-disclosed the revocation of warrants due to errors on the warrants. In both instances, the relevant investigators were informed and appropriate legal advice was sought to ensure that new warrants were issued.

The Ombudsman further noted one instance where the AFP self-disclosed that a warrant was not in the prescribed form. The Ombudsman states that the AFP identified the error, revoked the warrant and obtained a new warrant.

Further information about the Commonwealth Ombudsman's telecommunications interception inspection criteria is outlined in Figure 3 and 4 below.

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 Attorney-General 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 AGD) (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 obtained 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)).

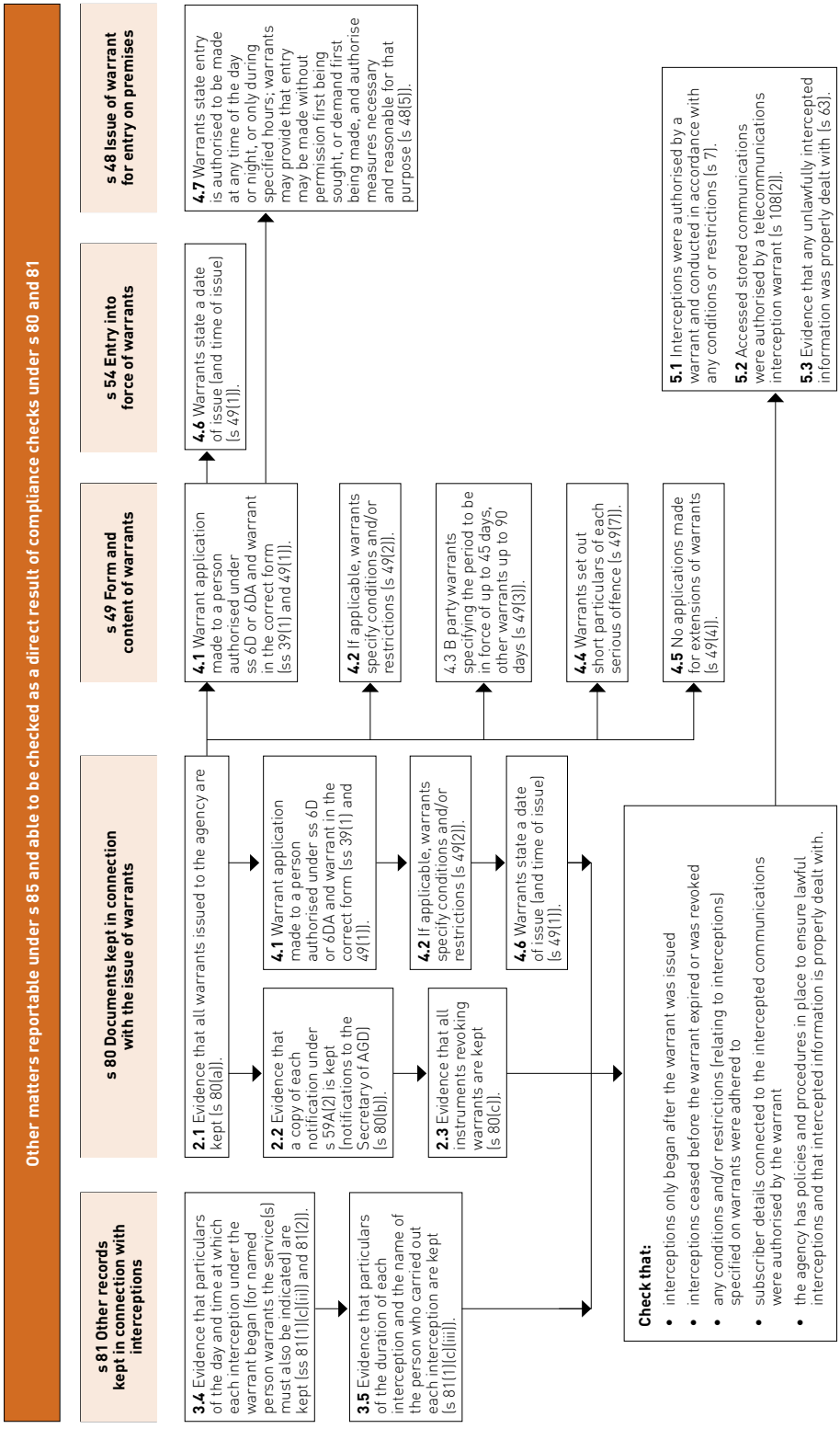
3.10 Evidence that particulars of each other agency from or to which or other person from or to whom the agency received or supplied the restricted record are kept (s 81(1)(d)(iv)).

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 s.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 Australian Competition and Consumer Commission.

Stored communications include communications such as email, SMS or voice messages stored on 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 three years**
- **offences punishable by a fine of least 210 penalty units (currently $37,800) for individuals or 900 penalty units (currently $189,000) for non-individuals such as corporations.**

Table 24: Applications and telephone applications for stored communications warrants—ss. 162(1)(a)-(b) and 162(2)(a)-(b)

Agency	Relevant statistics	Applications for stored communications warrants		Telephone applications for stored communications warrants	
		15/16	16/17	15/16	16/17
ACIC	Made	2	3	-	-
AFP	Made	80	50	-	-
ASIC	Made	1	-	-	-
CCC (QLD)	Made	3	13	-	-
CCC (WA)	Made	5	2	-	-
DIBP	Made	1	13	-	-
IBAC	Made	-	2		
ICAC (SA)	Made	-	3	-	-
LECC	Made	16	1	-	-
NSW CC	Made	4	2	-	-
NSW Police	Made	345	335	-	2
NT Police	Made	11	5	-	2
QLD Police	Made	132	92	-	-
SA Police	Made	19	12	-	-
TAS Police	Made	17	49	-	-
VIC Police	Made	41	58	-	-
WA Police	Made	35	34	**-**	**-**
TOTAL	**Made**	**712**	**674**	**-**	**2**
	Refused	**-**	**-**	**-**	**-**
	Issued	**712**	**674**	**-**	**2**

Table 25: Stored communications warrants subject to conditions or restrictions—s. 162(2)(d)

Agency	Application for warrants	
	15/16	16/17
NSW Police	345	335
SA Police	2	12
TOTAL	**347**	**347**

Effectiveness of stored communications warrants

In 2016–17, criminal law enforcement agencies made 394 arrests, conducted 1,064 proceedings and obtained 442 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—s. 163(a)-(b)

Agency	Arrests		Proceedings		Convictions	
	15/16	16/17	15/16	16/17	15/16	16/17
ACCC	-	-	1	-	-	-
ACIC	4	-	-	-	-	-
AFP	12	14	7	11	5	2
CCC (QLD)	2	-	1	-	1	-
ICAC (SA)	-	3	-	-	-	-
LECC	2	-	7	-	4	-
NSW CC	3	-	-	-	-	-
NSW Police	167	269	362	940	86	320
NT Police	7	5	7	2	2	2
QLD Police	130	48	67	78	66	78
SA Police	6	3	-	7	2	8
TAS Police	5	-	-	-	-	-
VIC Police	20	38	29	26	26	29
WA Police	8	14	4	-	3	3
TOTAL	**366**	**394**	**485**	**1,064**	**195**	**442**

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 or an even later reporting period.

Preservation notices

Under Part 3-1A of Chapter 3 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 decides not to apply for a warrant to access the stored communications.

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

Table 27: Domestic preservation notices—s. 161A(1)

Agency	Domestic preservation notice issued	Domestic preservation revocation notices issued
ACIC	3	2
AFP	100	22
CCC (QLD)	14	1
CCC (WA)	3	1
DIBP	102	9
IBAC	7	2
ICAC (NSW)	1	-
ICAC (SA)	24	11
LECC	1	-
NSW CC	5	-
NSW Police	478	80
NT Police	99	80
QLD Police	255	131
SA Police	73	42
TAS Police	150	33
VIC Police	106	29
WA Police	91	31
TOTAL	**1,512**	**474**

Under section 161A(2) of the TIA Act, the AFP is required to report on foreign preservation notices. In 2016–17, the AFP reported that 19 foreign preservation notices were issued with no revocations.

Mutual assistance

Section 162(1)(c) requires the report to outline the number of stored communications warrants obtained to assist in mutual assistance applications. No stored communications warrants were obtained in these circumstances during the reporting period.

Section 163A of the TIA Act provides 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 2016–17 there were no 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 records 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 will no longer include information on inspections concerning stored communications and preservation notices. Under new 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 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

An 'enforcement agency' includes all interception agencies as well as a body whose functions include administering a law imposing a pecuniary penalty or administering a law relating to the protection of the public revenue.

From 13 October 2015, the definition of enforcement agency was 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.

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.

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.

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 once the relevant telecommunications service provider receives the request and is effective for 45 days or less.

Existing data – enforcement of a criminal law

Tables 28 and 29 provide 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—s. 186(1)(a)

Agency	Authorisations	
	15/16	16/17
ACCC	70	53
ACIC	8721	8177
ACLEI	2,123	629
AFP	25,640	22,127
ASIC	1,822	1,677
CCC (QLD)	2,377	2,993
CCC (WA)	664	171
DIBP	2,622	3,337
IBAC	240	277
ICAC (NSW)	261	207
ICAC (SA)	112	306
LECC	1,479	339
NSW CC	2,196	2,322
NSW Police	105,710	104,176
NT Police	2,882	2,308
QLD Police	29,271	22,189
SA Police	14,264	6,060
TAS Police	7,969	9,162
VIC Police	82,034	82,041
WA Police	35,350	24,518
TOTAL	**325,807**	**293,069**

Table 29: Total number of authorisations made for access to existing information or documents in the enforcement of a criminal law—s. 186(1)(a)

Agency	Authorisations	
	15/16	16/17
No. of authorisations made by a commonwealth enforcement agency*	-	293,069
No. of authorisations made by a law enforcement agency	321,293	-
No. of authorisations made by a commonwealth agency	4,656	-
No. of authorisations made by a state or territory agency	424	-
TOTAL	**326,373**	**293,069**

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

Tables 30 and 31 provide information on the use of historical data authorisations to enforce a law imposing a pecuniary penalty or protecting public revenue.

Table 30: 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 the protection of the public revenue—s. 186(1)(b)

Agency	Authorisations	
	15/16	16/17
ACCC	62	10
AFP	75	38
ASIC	110	101
DIBP	67	32
IBAC	1	-
NSW Police	972	1,284
NT Police	4	2
QLD Police	70	4
SA Police	1	4
TAS Police	972	1,124
WA Police	92	8
TOTAL	**2,426**	**2,607**

* FFrom 13 October 2015, the definition of enforcement agency was restricted to 20 agencies that also fall under the definition of 'criminal law enforcement agency' (as set out in section 110A of the TIA Act). The data will be represented in the annual report under the category 'No. of authorisations made by a Commonwealth Enforcement Agency'.

Table 31: Total number of authorisations made for access to existing information or documents in the enforcement of a law imposing a pecuniary penalty or protecting public revenue—s. 186(1)(b)

Agency	Authorisations	
	15/16	16/17
No. of authorisations made by a commonwealth enforcement agency	-	2,597
No. of authorisations made by a law enforcement agency	2,187	-
No. of authorisations made by a commonwealth agency	339	-
No. of authorisations made by a state or territory agency	675	-
TOTAL	**3,201**	**2,607**

Existing data—assist in locating a missing person

Table 32 provides information on the use of historical data authorisations for the location of a missing person.

Table 32: Number of authorisations made for access to existing information or documents for the location of missing persons—s. 186(1)(aa)

Agency	Authorisations	
	15/16	16/17
AFP	96	91
NSW Police	1,597	1,197
NT Police	12	19
QLD Police	796	578
SA Police	147	63
TAS Police	175	1,092
VIC Police	1,513	1,256
WA Police	70	252
TOTAL	**4,406**	**4,548**

Prospective data—authorisations

Tables 33 and 34 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 33. 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 33: Prospective data authorisations—s. 186(1)(c)

Agency	Number of authorisations made	Days specified in force	Actual days in force	Authorisations discounted
ACIC	1,659	45,656	31,743	89
ACLEI	91	3,920	2,712	20
AFP	3,045	115,920	68,907	242
CCC (QLD)	355	9,538	7,221	17
CCC (WA)	92	3,996	2,391	21
DIBP	238	561	504	-
IBAC	139	5,516	3,804	24
ICAC (NSW)	7	315	196	1
ICAC (SA)	34	1,503	1,000	-
LECC	16	716	665	-
NSW CC	796	33,378	26,100	84
NSW Police	1,042	23,987	17,085	40
NT Police	401	13,055	10,292	2
QLD Police	3,453	148,868	110,406	336
SA Police	316	11,340	7,985	24
TAS Police	177	7,965	4,363	3
VIC Police	7,647	145,424	132,132	531
WA Police	1,032	42,757	28,867	87
TOTAL	**20,540**	**614,415**	**456,373**	**1521**

Table 34 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 2015–16 and 2016–17.

Table 34: Average specified and actual time in force of prospective data authorisations

Agency	Average period specified		Average period actual	
	15/16	16/17	15/16	16/17
ACIC	19	27	15	20
ACLEI	38	43	38	38
AFP	38	38	24	24
CCC (QLD)	26	26	15	21
CCC (WA)	43	43	35	33
DIBP	1	2	1	2
IBAC	42	39	36	33
ICAC (NSW)	45	45	23	32
ICAC (SA)	40	44	39	29
LECC	42	44	38	41
NSW CC	41	41	37	36
NSW Police	27	23	22	17
NT Police	44	32	38	25
QLD Police	43	43	40	35
SA Police	40	35	29	27
TAS Police	44	45	33	25
VIC Police	20	19	15	18
WA Police	45	41	30	30
AVERAGE	**35**	**35**	**28**	**27**

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 2016–17, the AFP made 47 data authorisations for access to telecommunications data for the enforcement of the criminal law of a foreign country.

Following these requests, the AFP made 18 disclosures to foreign law enforcement agencies. Information was disclosed to the following countries: New Zealand, South Africa and Taiwan.

Further reporting requirements

Tables 35 and 36 set out the offences for which authorised officers 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 35: Offences for which authorisations were made to access existing data to enforce the criminal law —s. 186(1)(e) [10]

Categories of offences	ACCC	ACIC	ACLEI	AFP	ASIC	CCC (QLD)	CCC (WA)	DIBP	IBAC	ICAC (NSW)	ICAC (SA)	LECC	NSW CC	NSW Police	NT Police	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Abduction	-	-	-	559	-	-	-	-	15	-	-	11	-	6,853	125	1,680	402	58	3,649	2,474	**15,826**
ACC investigation	-	8,177	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	**8,178**
Acts - injury	-	-	-	97	-	-	-	-	-	-	-	-	-	4,405	46	7	117	300	6,800	910	**12,682**
Bribery or corruption	-	-	629	340	-	333	171	-	143	100	303	221	-	2	32	-	803	-	304	1,186	**4,567**
Cartel offences	53	-	-	38	-	-	-	-	-	-	-	-	-	14	-	-	-	-	1	-	**106**
Conspire	-	-	-	55	17	-	-	-	-	-	-	-	-	109	-	-	11	233	332	94	**851**
Cybercrime	-	-	-	1,924	-	27	-	-	-	-	-	-	-	2,930	28	487	13	116	529	257	**6,311**
Dangerous acts	-	-	-	192	-	-	-	-	-	-	-	-	-	1,163	83	1134	277	-	534	68	**3,451**
Fraud	-	-	-	1,268	559	26	-	1182	80	104	3	36	840	10,902	105	794	319	438	1,264	936	**18,856**
Homicide	-	-	-	281	-	-	-	-	-	-	-	-	376	15,172	160	1,170	765	602	12,285	2,547	**33,358**
Illicit drug offences	-	-	-	12,362	-	1,796	-	1,863	12	-	-	53	755	24,582	1,121	5,451	1,250	2,825	11,273	8,341	**71,684**
Loss of life	-	-	-	21	-	-	-	-	-	-	-	-	-	538	25	444	7	-	5,205	18	**6,258**
Miscellaneous	-	-	-	254	1192	807	-	18	6	-	-	-	-	3,974	93	5,590	108	66	5,532	400	**18,040**
Justice procedures	-	-	-	154	7	-	-	-	13	-	-	18	1	630	8	-	62	82	535	249	**1,759**

10 Appendix F contains a description of each of the categories of offences.

Categories of offences	ACCC	ACIC	ACLEI	AFP	ASIC	CCC (QLD)	CCC (WA)	DIBP	IBAC	ICAC (NSW)	ICAC (SA)	LECC	NSW CC	NSW Police	NT Police	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Organised offences	-	-	-	350	-	-	-	-	-	-	-	-	-	1,236	5	-	2	-	3,026	275	**4,894**
Pecuniary penalty	-	-	-	51	-	-	-	-	-	-	-	-	-	506	3	-	-	20	-	-	**580**
Public revenue	-	-	-	30	-	-	-	-	-	-	-	-	-	-	-	-	1	-	-	-	**31**
People smuggling	-	-	-	171	-	-	-	-	-	-	-	-	-	-	-	-	1	-	-	2	**174**
Weapons	-	-	-	401	-	-	-	179	-	-	-	-	5	2,023	-	41	52	4	6,884	213	**9,802**
Property damage	-	-	-	60	-	-	-	-	-	-	-	-	4	1,462	14	-	400	-	4,900	-	**6,840**
Public order offences	-	-	-	7	-	-	-	-	-	-	-	-	-	56	-	49	-	-	-	12	**124**
Robbery	-	-	-	345	1	-	-	-	-	-	-	-	5	9,615	164	1,128	298	230	4,155	1,586	**17,527**
Serious damage	-	-	-	142	-	-	-	-	-	-	-	-	94	718	8	338	28	248	1,340	426	**3,342**
Sexual assault	-	-	-	574	-	3	-	12	-	-	-	-	1	7,522	99	1,150	581	808	2,354	1,286	**14,390**
Terrorism offences	-	-	-	1,561	-	1	-	8	-	-	-	-	240	1,336	4	-	70	-	453	313	**3,986**
Theft	-	-	-	768	6	-	-	75	8	3	-	-	1	5,389	128	1,106	271	2,031	5,274	1,061	**16,121**
Traffic	-	-	-	27	-	-	-	-	-	-	-	-	-	691	9	136	9	1	198	108	**1,179**
Unlawful entry	-	-	-	95	-	-	-	-	-	-	-	-	-	2,259	48	1,484	213	1,100	5,214	1,755	**12,168**
TOTAL	**53**	**8,177**	**629**	**22,127**	**1,782**	**2,993**	**171**	**3,337**	**277**	**207**	**306**	**339**	**2,322**	**104,087**	**2,308**	**22,189**	**6,060**	**9,162**	**82,041**	**24,518**	**293,085**

Table 36: 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—s. 186(1)(e) [11]

Categories of offences	ACCC	AFP	ASIC	DIBP	NSW Police	NT Police	QLD Police	SA Police	TAS Police	WA Police	TOTAL
Abduction	-	-	1	-	127	-	-	-	17	1	**146**
Acts - injury	-	-	-	-	21	-	-	-	82	-	**103**
Cybercrime	-	-	-	-	17	-	-	-	66	-	**83**
Dangerous acts	-	-	-	-	9	-	-	-	-	-	**9**
Fraud	10	12	90	7	67	-	-	-	6	-	**192**
Homicide	-	-	-	-	77	-	-	-	-	-	**77**
Illicit drug offences	-	4	-	8	95	-	-	-	-	-	**107**
Loss of life	-	-	-	-	3	-	-	-	-	-	**3**
Miscellaneous	-	1	38	1	55	2	1	-	18	-	**116**
Justice procedures	-	4	3	-	-	-	-	-	130	-	**137**
Organised offences	-	-	-	-	31	-	-	-	-	-	**31**
Pecuniary penalty	-	5	1	7	553	-	-	4	516	-	**1,086**
Public revenue	-	9	-	-	-	-	-	-	-	-	**9**
Weapons	-	-	-	8	16	-	-	-	146	-	**170**

11 Appendix F contains a description of each of the categories of offences.

Categories of offences	ACCC	AFP	ASIC	DIBP	NSW Police	NT Police	QLD Police	SA Police	TAS Police	WA Police	TOTAL
Pollution	-	-	-	-	13	-	-	-	-	-	**13**
Public order	-	-	-	-	3	-	-	-	-	-	**3**
Robbery	-	-	-	-	67	-	-	-	-	-	**67**
Serious damage	-	-	-	-	5	-	-	-	-	-	**5**
Sexual assault	-	-	-	-	39	-	3	-	-	-	**42**
Terrorism offences	-	-	-	-	8	-	-	-	-	-	**8**
Theft	-	3	-	1	32	-	-	-	111	-	**147**
Traffic	-	-	-	-	43	-	-	-	31	7	**81**
Unlawful entry	-	-	-	-	5	-	-	-	1	-	**6**
TOTAL	**10**	**38**	**133**	**32**	**1,286**	**2**	**4**	**4**	**1,124**	**8**	**2,641**

Table 37: 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—s. 186(1)(e) [12]

Categories of offences	ACIC	ACLEI	AFP	CCC (QLD)	CCC (WA)	DIBP	IBAC	ICAC (NSW)	ICAC (SA)	LECC	NSW CC	NSW Police	NT Police	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Abduction	-	-	32	-	-	-	1	-	-	-	1	21	12	26	51	5	821	36	**1,006**
ACC investigation	1,659	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**1,659**
Acts - injury	-	-	13	-	-	-	-	-	-	-	-	40	15	104	15	-	268	41	**496**
Bribery or corruption	-	91	21	20	92	-	84	3	33	11	-	-	7	9	-	-	5	21	**397**
Cartel offences	-	-	13	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**13**
Conspire	-	-	3	-	-	-	-	-	1	-	-	12	-	8	1	6	31	16	**78**
Cybercrime	-	-	76	2	-	-	-	-	-	-	-	3	1	-	-	5	15	-	**102**
Dangerous acts	-	-	7	-	-	-	-	-	-	-	-	4	2	16	5	-	954	6	**994**
Fraud	-	-	158	1	-	124	39	4	-	2	252	20	6	100	-	1	89	6	**802**
Homicide	-	-	23	-	-	-	-	-	-	-	105	30	4	175	12	19	946	30	**1,344**
Illicit drug offences	-	-	1,823	225	-	90	10	-	-	-	216	480	280	2,561	166	76	905	541	**7,373**
Loss of life	-	-	2	-	-	-	-	-	-	-	-	44	-	4	-	-	211	-	**261**
Miscellaneous	-	-	37	105	-	-	-	-	-	-	-	62	4	16	4	-	393	4	**625**
Justice procedures	-	-	9	-	-	-	-	-	-	3	-	1	-	-	4	2	37	2	**58**
Organised offences	-	-	105	-	-	-	-	-	-	-	-	21	1	7	5	-	325	-	**464**

12 Appendix F contains a description of each of the categories of offences.

Categories of offences	ACIC	ACLEI	AFP	CCC (QLD)	CCC (WA)	DIBP	IBAC	ICAC (NSW)	ICAC (SA)	LECC	NSW CC	NSW Police	NT Police	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Pecuniary penalty	-	-	3	-	-	-	-	-	-	-	-	-	-	-	-	3	-	2	**8**
Public revenue	-	-	5	-	-	-	-	-	-	-	-	5	-	-	-	-	3	-	**13**
People smuggling	-	-	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**2**
Weapons	-	-	90	-	-	12	-	-	-	-	8	83	-	45	1	1	141	23	**404**
Pollution	-	-	4	-	-	-	-	-	-	-	-	5	-	8	7	-	48	-	**72**
Public order offences	-	-	5	-	-	-	-	-	-	-	-	-	-	-	-	-	3	-	**8**
Robbery	-	-	14	-	-	-	-	-	-	-	-	103	36	129	16	6	417	81	**802**
Serious damage	-	-	-	-	-	-	-	-	-	-	24	1	2	4	2	5	207	12	**257**
Sexual assault	-	-	26	-	-	-	-	-	-	-	-	23	2	33	2	8	782	7	**883**
Terrorism offences	-	-	189	-	-	-	-	-	-	-	190	14	0	1	2	-	168	7	**573**
Theft	-	-	55	-	-	12	5	-	-	-	-	47	9	25	6	7	461	15	**642**
Traffic	-	-	4	-	-	-	-	-	-	-	-	-	5	-	2	1	-	20	**32**
Unlawful entry	-	-	8	-	-	-	-	-	-	-	-	23	15	182	29	33	417	162	**869**
TOTAL	**1,659**	**91**	**2,727**	**355**	**92**	**238**	**139**	**7**	**34**	**16**	**796**	**1,042**	**401**	**3,453**	**330**	**178**	**7,647**	**1,032**	**20,237**

Table 38 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 was made. The statistics are spilt into successive periods of 3 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, 79 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,[13] 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.

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

Table 38: Periods which retained data was held by carrier before authorised disclosure—s. 186(1)(f)

Agency	Age of data under disclosure									
	0-3 mths.	3-6 mths.	6-9 mths.	9-12 mths.	12-15 mths.	15-18 mths.	18-21 mths.	21-24 mths.	Over 24 mths.	**TOTAL**
ACCC	16	-	23	5	-	1	-	5	13	**63**
ACIC	7,743	216	75	77	41	5	13	4	9	**8,183**
ACLEI	33	25	29	14	14	8	5	2	120	**250**
AFP	15,250	2,782	1032	1,167	560	195	199	238	864	**22,287**
ASIC	1,534	27	18	21	15	16	3	14	53	**1,701**
CCC (QLD)	1,816	663	186	101	107	66	29	8	17	**2,933**
CCC (WA)	263	-	-	-	-	-	-	-	-	**263**
DIBP	2,743	393	158	128	68	18	15	8	76	**3,607**
IBAC	221	17	7	-	6	7	2	5	12	**277**
ICAC (NSW)	67	20	12	8	6	38	8	0	48	**207**
ICAC (SA)	77	51	50	50	31	5	-	1	14	**279**
LECC	282	27	21	8	-	-	-	1	-	**339**
NSW CC	1,624	145	67	85	28	59	33	66	215	**2,322**
NSW Police	93,366	5,763	2,637	1,255	1,191	432	337	362	1,314	**106,657**
NT Police	2,439	-	-	-	-	-	-	-	-	**2,439**
QLD Police	17,341	1,633	1,074	572	505	264	191	98	624	**22,302**
SA Police	3,890	822	290	490	89	64	75	78	343	**6,141**
TAS Police	3,156	467	164	81	43	26	9	9	150	**4,105**
VIC Police	61,131	6,712	5,691	3,497	2,579	2,486	1,134	47	20	**83,297**
WA Police	17,184	2,731	1,507	1,211	638	401	270	192	644	**24,778**
TOTAL	**230,176**	**22,494**	**13,041**	**8,770**	**5,921**	**4,091**	**2,323**	**1138**	**4,536**	**292,463**

Table 39 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 includes information identifying the user of a telecommunications service. Data within items 2-6 of that subsection are typically considered 'traffic data' and include information such as the time, duration and source of a communication.[14]

Table 39: Types of retained data disclosed in authorisations—ss. 186(1)(g) and 186(1)(h)

Agency	Number of authorisations which included information from the data sets identified in subsection 187AA(1)		
	Item 1: subscriber data	Items 2-6: traffic data	**TOTAL**
ACCC	53	10	**63**
ACIC	5,485	2,692	**8,177**
ACLEI	464	165	**629**
AFP	6,179	16,086	**22,265**
ASIC	1,441	260	**1,701**
CCC (QLD)	2,381	612	**2993**
CCC (WA)	142	121	**263**
DIBP	2,834	1,005	**3,839**
IBAC	203	76	**279**
ICAC (NSW)	93	114	**207**
ICAC (SA)	137	169	**306**
LECC	240	115	**355**
NSW CC	1,539	1,070	**2,609**
NSW Police	81,613	25,044	**106,657**
NT Police	2,329	110	**2,439**
QLD Police	16,645	8,548	**25,193**
SA Police	4,035	2,111	**6,146**
TAS Police	9,954	1,424	**11,378**
VIC Police	60,515	22,782	**83,297**
WA Police	19,712	5,066	**24,778**
TOTAL	**215,994**	**87,580**	**303,574**

14 Appendix E further explains the type of data included 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 no authorisations were made under JIWs.[15]

Industry estimated cost of implementing data retention obligations

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 three financial years commencing July 2014 and ending June 2017 (set out in table 44).

Table 44 further sets out the costs recovered from criminal law enforcement agencies (CLEAs) for the purpose of complying with their data retention obligations.

Table 40: Industry Capital Costs of data retention—s. 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
Total	**$176,192,834.17**	**$26,558,256.64**

During the reporting period, the total funding provided under the Data Retention Industry Grants Programme was $131,593,265.57 (GST inclusive). There were 174 recipients of this funding.

15 The Attorney-General tabled 'A report on the Commonwealth Ombudsman's inspection of the Australian Federal Police under the Telecommunications (Interception and Access) Act 1979—Access to journalist's telecommunications data without a journalist information warrant' in the Senate on 28 November 2017 and the House of Representatives on 4 December 2017

Use of data retention plans

The Data Retention Act came into effect on 13 October 2015 and providers were able to apply to the Communications Access Coordinator for an additional 18 months to comply with the legislation through an approved Data Retention Implementation Plan. During the 18 month implementation period which ended on 13 April 2017, the Attorney-General's Department received 402 Data Retention Implementation Plans from 310 providers. The plans were assessed by the Communications Access Co-ordinator in accordance with the process in section 187F of the Act, including consultation with agencies and the Australian Communications Media Authority under section 187G.

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

LIST OF TABLES AND FIGURES

Tables

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
Corruption and Crime 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
ATO	Australian Taxation Office
CAC	Communications Access Co-ordinator
CCC (WA)	Corruption and Crime Commission (Western Australia)
CCC (QLD)	Crime and Corruption Commission (Queensland)
DIBP	Former Department of Immigration and Border Protection (including the Australian Customs and Border Protection Service)
Defence (IGD, ADFIS)	Inspector-General Defence, Australian Defence Force Investigative Service
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
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)
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; ii) any other information for identification purposes; relating to the relevant service, being information used by the service provider for the purposes of identifying the subscriber of the relevant service; (b) any information relating to any contract, agreement or arrangement relating to the relevant account, service or device; (c) any information that is one or both of the following: (i) billing or payment information; (ii) contact information; relating to the relevant service, being information used by the service provider in relation to the relevant service; (d) any identifiers relating to the relevant service or any related account, service or device, being information used by the service provider in relation to the relevant service or any related account, service or device; (e) the status of the relevant service or any related account, service or device	This category includes customer identifying details, such as name and address. It also includes contact details, such as phone number and email address. This information allows agencies to confirm a subscriber's identity or link a service or account to a subscriber. This category also includes details about services attached to 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, or • any other service or device identifier known to the provider that uniquely identifies the source of the communication. In all instances, the identifiers retained to identify the source of the communication are the ones relevant to, or used in, the operation of the particular service in question.

Item	Description of information	Explanation
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 (examples 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, or • 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, and d) the disconnection from the relevant service.	For phone calls this is simply the time a call started and ended. For internet sessions this is when a device or account connects to a data network and ends when it disconnected – those events may be a few hours to several days, weeks, or longer apart, depending on the design and operation of the service in question.

Item	Description of information	Explanation
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 enable for the communication. Examples: call waiting, call forwarding, data volume usage.	The type of communication means the form of the communication (for example voice call vs. internet usage). The type of the relevant service (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 187A(4)(e) of the Bill 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 locations 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 vehicle regulatory offences
Unlawful entry	Unlawful entry with intent/burglary, break and enter