Pages 1 through 2 redacted for the following reasons:
---
s47E(d)

s47E(d)

Journalist Information Warrant

An Authorising Officer **must not** make an authorisation under section 178, 178A, 179 or **180** of the Act without a **Journalist Information Warrant** if there is a reasonable belief the particular person subject of the disclosure is;

i. working in a professional capacity as a journalist; or
ii. an employer of such a person; and

a purpose of the authority would be to identify a possible source.

s47E(d)

*For information on **Journalist Information Warrants** refer to* Data Retention on the Investigators Toolkit

Operational Information	
Target Name	(enter target's name – surname in CAPITALS)
Operation Name	(enter Operation name)
PROMIS No.	(enter Promis No.)
IPND/Subscriber	(select response & attach copy)

Applicant/ Requesting Officer	(enter name & service number)	**Contact Number**	(enter contact number)
Function	(select function)	**Region**	(select region)
Secondary Contact Officer	(enter name & service number)	**Contact Number**	(enter contact number)

s47G(1)

s47G(1)

s47E(d)

Refer Carrier Connection Fees, s47G(1)

After Hours Connections must be approved by Coordinator TID prior to request	
A/H Approved	(select response)
Cost Centre	(enter cost centre)

Once form is signed or electronically approved by an Authorised Officer, scan and/or email to s22(1)(a)(ii)

Pages 5 through 11 redacted for the following reasons:
---
s22(1)(a)(ii)

s22(1)(a)(ii)

Data Authorisations

Telecommunications data, or metadata, is information about a communication which does not include its content. In the example of a phone call, metadata may include the phone numbers of the two parties to the conversation, the duration, date, time and location of that phone call but not what was said.

Communication content is separate to telecommunications data. Examples of communication content include any information that reveals the substance of a communication, such as the body and subject line of an email, the text within an SMS, the audio of a call, private social media posts, or what a subscriber searched for online (URLs). A warrant is still required to access the content of a communication.

There are two types of internally issued data authorisations, or requests for metadata:

Historical telecommunications

Request authorises disclosure of existing information such as, Integrated Public Number Database(IPND), subscriber checks, Call Charge Records (CCR), Reverse CCR, internet data

Prospective telecommunications

Requests such as s47E(d) s47G(1) s47G(1)

IMPORTANT: 180F Authorised officers to consider privacy

Before making an authorisation under Division 4 or 4A in relation to the disclosure or use of information or documents, the authorised officer considering making the authorisation must be satisfied on reasonable grounds that any interference with the privacy of any person or persons that may result from the disclosure or use is justifiable and proportionate, having regard to the following matters:

(aa) the gravity of any conduct in relation to which the authorisation is sought, including:

(i) the seriousness of any offence in relation to which the authorisation is sought; and

(ii) the seriousness of any pecuniary penalty in relation to which the authorisation is sought; and

(iii) the seriousness of any protection of the public revenue in relation to which the authorisation is sought; and
(iv) whether the authorisation is sought for the purposes of finding a missing person;

(a) the likely relevance and usefulness of the information or documents;
(b) the reason why the disclosure or use concerned is proposed to be authorised.

Data Authorisations – Historic

Chapter 4 of the TIA Act outlines how enforcement agencies may access information or documents held by a telecommunications carrier that exist at the time of the request. An authorisation enables carriers to lawfully disclose information or documents, such as customer details, call records and cell data, to the authorising agency.

When is access to historic telecommunications data permitted?

Primary Disclosure (for the AFP)

Section 178 - Authorisations for access to existing information or documents — enforcement of the criminal law

Permitted where it is reasonably necessary for the enforcement of Australian criminal law.

Section 178A - Authorisations for access to existing information or documents—locating missing persons

Permitted where it is reasonably necessary to locate a person who police have been notified is missing.

Section 179 - Authorisations for access to existing information or documents—enforcement of a law imposing a pecuniary penalty or protection of the public revenue

Permitted where it is reasonably necessary for the enforcement of an Australian law that imposes a pecuniary penalty or for the protection of public revenue.

Section 180A - Authorisations for access to existing information or documents — enforcement of the criminal law of a foreign country

Permitted where it is reasonably necessary for the enforcement of the criminal law of a foreign country. Additionally,180A(4) allows disclosure of information obtained under 180A to a foreign law enforcement agency where it is reasonably necessary for the enforcement of the criminal law of a foreign country and appropriate in all the circumstances.

Secondary Disclosure (for the AFP to release to foreign law enforcement agencies)

Section 180C - Authorisations to disclose information or documents — enforcement of the criminal law of a foreign country

Allows the disclosure of information to a foreign law enforcement agency that has already been obtained under an authorisation under Division 4, with the exception of 178A (missing persons). The disclosure must be reasonably necessary for the enforcement of the criminal law of a foreign country and appropriate in all the circumstances.

Section 180D - Authorisations to disclose information or documents — enforcement of the criminal law

Allows the disclosure of information to s7(1) or an Australian enforcement agency obtained under Division 4A(foreign law enforcement).

Not all policing activities or investigations fit within the scope of permitted access to historic telecommunications data. If in doubt, seek advice.

- Authorisations under section 178, 178A and 179 **must** be authorised by the Commissioner, a Deputy Commissioner or a person who is an authorised officer under section 5AB(1). This means sworn members at the rank of Assistant Commissioner, Commander, Superintendent and Officer in Charge (ACT Policing Intelligence Band 8).
- Authorisations under section 180A, 180C and 180D **must** be authorised by the Commissioner, a Deputy Commissioner or a person who is an authorised officer under section 5AB(1A). This means a senior executive AFP employee who is a member of the AFP holding the rank of Assistant Commissioner or Commander.

Historic data requests relating to the enforcement of a criminal law of a foreign country

The TIA Act allows the AFP to obtain historical telecommunications data and pass that data on to a foreign law enforcement agency without the need for a Mutual Assistance Request.

If the AFP has not previously obtained the information under s178 or s179 follow this process (i.e., the information is being obtained for the purpose of the enforcement of the criminal law of a foreign country and not for a domestic purpose):

Under s180A(2), an AFP authorised officer authorises the release of information from the telecommunications provider to the AFP; and

Under s180A(4), an AFP authorised officer authorises the release of information from the AFP to a foreign law enforcement agency if the authorised officer is satisfied that:

a. The disclosure is reasonably necessary for the enforcement of the criminal law of a foreign country; and
b. The disclosure is appropriate in all the circumstances.

Members should also consider whether the matter in which data is to be provided to the foreign law enforcement agency is a matter to which the* AFP National Guideline on international police-to-police assistance in death penalty situations *applies.

If the AFP has previously obtained the information under s178 or s179 that information may be provided to the foreign law enforcement agency under:

s180C – secondary disclosure for the enforcement of a criminal law of a foreign country.

Data obtained for a foreign law enforcement purpose can be used or disclosed for a domestic purpose under s180D.

For further information, please see the Foreign Disclosures sections on the Data Retention toolkit page.

Subject to the requirements of the foreign country, an MAR may be required if the requested information is required in court proceedings.

Data Authorisations – Prospective

Overview

Prospective data[4]request authorisation may be given pursuant to s180 of the *Telecommunications (Interception and Access) Act 1979* (TIA Act). Section 180(2) of the TIA Act provides that an authorised officer of a criminal law-enforcement

[4] Prospective data refers to information or documents that come into existence during the period for which the authorisation is in force. This means the data can be obtained on an ongoing or prospective basis. s47E(d)

agency may authorise the disclosure of specified information or documents that **come into existence** during the period for which the authorisation is in force.

When is access to prospective telecommunications data permitted?

As the authorised officer, you must not make the authorisation unless you are satisfied the disclosure is reasonably necessary for the investigation of a "serious offence"; or an offence against a law of the Commonwealth, a State or a Territory that is punishable by imprisonment for at least 3 years.

How must a s180 authorisation be made?

Complete the electronic Section 180(2) Prospective Request Electronic form and email to TID Interception management Team for action with the carrier. The request must be made in writing utilising the request form and cannot be made verbally.

The link below takes you to the Investigator's Toolkit page.

Subsection 180(2) – Prospective Request Information

Prospective data disclosure to a foreign country

It is possible to disclose prospective telecommunications data to a foreign country. An authorised officer must not make a prospective data authorisation for the disclosure of information to the AFP under s 180B(2) unless:

- The AO is satisfied disclosure is appropriate in all the circumstances;
- The Attorney General has authorised the making of the authorisation under the Mutual Assistance in Criminal Matters Act 1987 (which in practice requires a mutual assistance request to have been made by the foreign country); and
- The AO is satisfied that the disclosure is reasonably necessary for the investigation of a "serious offence" or a law that is punishable by imprisonment for at least 3 years or involves an act or omission that, if it had occurred in Australia, would constitute a serious offence.

The AO can only make one s180B(8) authorisation per day to ensure the AFP reviews the information disclosed by the telecommunications provider each day before further disclosure to a foreign country.

s47E(d)

s47E(d)

Journalist Information Warrants

A Journalist Information Warrant (JIW) is required to permit access to telecommunications data i.e. the making of data 'Authorisations' relating to a person who is reasonably believed to be working in a professional capacity as a journalist, or to be the employer of such a person, **where a purpose for making the authorisation is to identify another person who is reasonably believed to be a journalist's source of information.**

Definition of Journalist

There is no definition of 'journalist' under the TIA Act. The TIA Act simply requires the person be working as a journalist in a professional capacity. Indicators that a person is acting in a professional capacity could include:

- regular employment
- adherence to enforceable ethical standards, and
- membership of a professional body.

Definition of Source

Section 5 of the TIA Act defines **source** as '… a person who provides information:

a. to another person who is working in a professional capacity as a journalist; and

b. in the normal course of the other person's work in such a capacity; and
c. in the expectation that the information may be disseminated in the form of:
    i. news, current affairs or a documentary; or
    ii. commentary or opinion on, or analysis of, news, current affairs or a documentary.

Obtaining a JIW differs from other warrants in a number of ways, including the ability of a Public Interest Advocate to make submissions to the issuing authority (Judge/AAT Member) on behalf of the relevant journalist, before the warrant is issued.

The AFP has amended the instrument of delegation relating to 'authorised officers' under the Act, such that only Commanders and above can make a data authorisation (under ss.178, 178A, 179 or 180) following the obtaining of a JIW.

The process to apply for a JIW is detailed in the Better Practice Guide on Procedures to obtain a Journalist Information Warrant.

As an Authorised Officer you must be aware of the following limitations prior to making an authorisation:

Domestic requests

An AO **must not** make an authorisation under section 178, 178A, 179 or 180 that would authorise the disclosure of information or documents relating to a particular person if the authorised officer knows or reasonably believes that particular person to be:

- a person who is working in a professional capacity as a journalist, **or**
- an employer of such a person, **and**
- a purpose of making the authorisation would be to identify another person who is known or reasonably believed to be a source unless a JIW is in force.

Note: A JIW **cannot** be obtained for Division 4A authorisations (ss.180A, 180B, 180C or 180D - in relation to access or disclosure of telecommunications data for a **foreign law enforcement agency**). Therefore, an authorisation cannot be made where the circumstances would otherwise require a JIW.

Further Information

If you are intending on applying for a journalist information warrant, contact your s47E(d) for advice beforehand s47E(d) s47E(d)

If a journalist is the subject of the investigation or **if there is any uncertainty about the need for a JIW contact AFP Legal** to obtain guidance s47E(d) s47E(d)

For further information please refer to the AGD Information Sheet (Journalistic Information Warrant) and the Journalist Information Warrant section on the Data Retention page.

s47E(d)

s47E(d)

s22(1)(a)(ii)

Pages 21 through 45 redacted for the following reasons:
---
s22(1)(a)(ii)

s22(1)(a)(ii)

Data Authorisations

Data Retention

Service providers who operate a service to which Part 5-1A of the TIA Act applies must keep certain records or information for at least 2 years.

Chapter 4 of the Act outlines how enforcement agencies may access metadata held by a telecommunications carrier. An internally issued authorisation enables carriers to lawfully disclose information or documents, including metadata to the agency. In certain circumstances, a journalist information warrant is also required before such authorisation may be given.

For more information on data retention and what constitutes metadata, please see the Data Retention page.

Authorisations **must** be issued before any disclosure of information.

Who can authorise data authorisations

Domestic requests: An authorised officer within the meaning of s 5AB(1) of the TIA Act. This is currently the Commissioner, Deputy Commissioner, Commanders, Superintendents and the person occupying the position of Officer in Charge of ACT Policing Intelligence.

Foreign requests: An authorised officer within the meaning of s 5AB(1A) of the TIA Act. This is currently individually named AFP SES members, as listed in the instrument.

Issuing Data Authorisations –Domestic

AFP Authorised Officers for domestic data authorisations

- s178, s178A, s179 – authorise disclosure of **historic information**
  - Subscriber checks, Integrated Public Number Database (IPND), Call Charge Records (CCR), Reverse CCR, Internet data
- s180 – authorise disclosure of **prospective information**
  - s47E(d) s47G(1) handset location

Issuing Data Authorisations -Foreign

AFP Authorised Officers for foreign data authorisations

- s180A – authorise disclosure of **historic information** for a foreign country

- Subscriber checks, IPND, CCR, Reverse CCR, Internet data
- s180B – authorise disclosure of **prospective information** for a foreign country
  - s47G(1) handset location
- s180C- authorise secondary disclosure of historic or prospective information previously obtained under s178, s179 (not s178A) and s180
- s180D- authorise disclosure of historic or prospective information previously obtained under a foreign data authorisation to s7(1) or Australian enforcement agency for the enforcement of criminal law

For further information, refer to the Part 4-1 and Part 4-2 instruments under the *Telecommunications (Interception and Access) Act 1979 (Cth)* within the Delegations and Authorisations Collection.

Restrictions

If a purpose of the data request is to **identify a source of a person who is working in a professional capacity as a journalist, or the employer of such a person,** a Journalist Information Warrant (JIW) **MUST** be applied for before any subsequent authorisations under ss178, 178A, 179 or 180 are applied for. This is covered in the next chapter of the course.

When is access to historic telecommunications data permitted?

- Section 178 – it is reasonably necessary for the enforcement of the criminal law
- Section 178A – it is reasonably necessary to locate a person whom police have been notified is missing
- Section 179 – it is reasonably necessary for the enforcement of an Australian law that imposes a pecuniary penalty or for the protection of Commonwealth public revenue
- Section 180A– it is reasonably necessary for the enforcement of a criminal law of a foreign country

Historic data requests relating to the enforcement of a criminal law of a foreign country

If the AFP has not previously obtained the information under s 178 or s 179 a two-step process must occur:

1. Under s180A(2), an AFP authorised officer authorises the release of information from the telecommunications provider to the AFP; and
2. Under s 180A(4), an AFP authorised officer authorises the release of information from the AFP to a foreign law enforcement agency if the authorised officer is satisfied that:
   a. The disclosure is reasonably necessary for the enforcement of the criminal law of a foreign country; and
   b. The disclosure is appropriate in all the circumstances.

If the AFP has previously obtained the information under s178 or s179 of that information may be provided to the foreign law enforcement agency under:

- s 180C – secondary disclosure for the enforcement of a criminal law of a foreign country.

For further information, please see the Foreign Disclosures sections on the Data Retention page.

When is access to prospective telecommunications data permitted?

- It is reasonably necessary for the investigation of a "serious offence"; or an offence against a law of the Commonwealth, a State or a Territory that is punishable by imprisonment for at least 3 years.
- The authorisation **must** be revoked when the disclosure of information is no longer required; or in a case where the authorisation is made under a journalist information warrant–the warrant is revoked

For further information, please see the Information for Requesting and Authorising Officers page.

Prospective data disclosure to a foreign country

It is possible to disclose prospective telecommunications data to a foreign country; however it is a more difficult process than for historical telecommunications data. An authorised officer must not make a prospective data authorisation for the disclosure of information to the AFP under s 180B(2) unless:

- The Attorney General has authorised the making of the authorisation under the *Mutual Assistance in Criminal Matters Act 1987*
- The AO is satisfied that the disclosure is reasonably necessary for the investigation of a "serious offence" or a law that is punishable by imprisonment for at least 3 years or involves an act or omission that, if it had occurred in Australia, would constitute a serious offence; and
- The AO to be satisfied disclosure is appropriate

- If information or documents are disclosed to the AFP pursuant to an authorisation provided under s 180B(2), an AFP authorised officer may authorise the disclosure of the information or documents to a foreign law enforcement agency if satisfied that:
  - The disclosure is reasonably necessary for the investigation of a "serious offence" or a law that is punishable by imprisonment for at least 3 years or involves an act or omission that, if it had occurred in Australia, would constitute a serious offence; and
  - It is appropriate in all the circumstances.

The AO can only make one s180B(8) authorisation per day to ensure the AFP reviews the information disclosed by the telecommunications provider each day before further disclosure to a foreign country.

What must an AO consider when approving telecommunications data requests?

When making data authorisations, AOs are required to **be satisfied on reasonable grounds** that any interference with the privacy of any person or persons that may result from the disclosure or use of the data is **justifiable and proportionate**, having regard to the following factors:

- The gravity of the conduct being investigated
- The likely relevance and usefulness of the information or documents; and
- The reason for the disclosure or use.

Records must be kept to demonstrate that authorisations were properly made. AOs need to be able to articulate their reasoning against these criteria if their decision is tested.

Refer to Guidance on new Privacy consideration.

How must an authorisation be made?

The authorising officer must approve the request **in writing** and must be signed (electronic or otherwise). There are legislative requirements setting out the form of the authorisation which must be adhered to.

Authorisations must not be made verbally.

Use and Disclosure of Telecommunications Data

Under section 182, telecommunications data that does not relate to a missing person (section 178A) may be lawfully used or disclosed when, among other things, it is reasonably necessary for the enforcement of the criminal law or for the enforcement of a law imposing a pecuniary penalty in accordance with section 180C and 180D.

For further information please refer to the Training and Reference Material and AGD Information Sheet (Use and Disclosure) on the Data Retention page on the Hub.

Records and Reports for historical and prospective telecommunications data requests

- The AFP must keep **records** in relation to telecommunication requests including:
    - Each authorisation and revocation instrument
    - Records that show whether the authorisation or revocation was properly made
    - Use and Disclosure of information obtained under Authorisation
    - Evidentiary Certificates

- The AFP must **report** to the Minister on the following:
    - Number of authorisations made
    - Number of authorisations made under a Journalist Information Warrant
    - Offences and other matters for which authorisations were made
    - Length of time for which the information had been held
    - The type of information or data sought
    - The name of each country and number of disclosures to each such country

Refer to AGD Information Sheet (Record-keeping and reporting)

Further Information

- Data Retention page on the Investigator's Toolkit
- AFP National Guideline telecommunications interception and accessing stored communications
- Telecommunications (Interception and Access) Act 1979
- Considerations for Authorising Officers
- Telecommunications Intercepts and Stored Communications page on the Investigator's Toolkit
- team on s47E(d)
- s47E(d) Team s47E(d)

Journalist Information Warrants and Authorisations

A Journalist Information Warrant (JIW) is required to permit access to telecommunications data (i.e. the making of data 'Authorisations') relating to a person (or employer of a person) who is reasonably believed to be working in a professional capacity as a journalist, where a purpose for making the authorisation is to identify another person who is reasonably believed to be a journalist's source of information.

The AFP has amended the instrument of delegation relating to 'authorised officers' under the Act, such that only Commanders and above can make a data authorisation (under ss. 178, 178A, 179 or 180) **following the obtaining of a JIW.**

Considerations

AOs **must be** aware of the following limitations prior to making an authorisation:

Domestic requests

An AO **must not** make an authorisation under section 178, 178A, 179 or 180 that would authorise the disclosure of information or documents relating to a particular person if the authorised officer knows or reasonably believes that particular person to be:

- a person who is working in a professional capacity as a journalist, or
- an employer of such a person, **and**

a purpose of making the authorisation would be to identify another person who is known or reasonably believed to be a source **unless** a JIW is in force.

Note: A JIW cannot be obtained for Division 4A authorisations (ss. 180A, 180B, 180C or 180D - in relation to access or disclosure of telecommunications data for a **foreign law enforcement agency**). Therefore, an authorisation cannot be made where the circumstances would otherwise require a JIW.JIWs have a more complicated process where a Public Interest Advocate may make submissions to the issuing authority (Judge/AAT Member) on behalf of a journalist before the warrant is issued.

The process to apply for a JIW is detailed in the Better Practice Guide on Procedures to obtain a Journalist Information Warrant.

For further information please refer to the AGD Information Sheet (Journalistic Information Warrant) and the Journalist Information Warrant section on the Data Retention page.

Who is authorised to issue a JIW?

Similar to other warrants available under the *Telecommunications (Interception and Access) Act 1979* (the Act), a Part 4-1 issuing authority within the meaning of the Act is able to issue a JIW.

The process to apply for a JIW is detailed in the Better Practice Guide on Procedures to obtain a Journalist Information Warrant.

Obtaining a JIW differs from other warrants in a number of ways, including the ability of a Public Interest Advocate to make submissions to the issuing authority (Judge/AAT Member) on behalf of the relevant journalist, before the warrant is issued.

For further information please refer to the AGD Information Sheet (Journalistic Information Warrant) and the Journalist Information Warrant section on the Data Retention page.

Other Requirements

- The Commissioner must, as soon as practicable, provide to the Minister and the Ombudsman:
  - A copy of the journalist information warrant
  - Any authorisations made under the warrant
- The Commissioner may revoke a JIW at any time and **must** do so if satisfied that the grounds on which the warrant was issued to the agency have ceased to exist. The Commissioner may delegate this power to a 'certifying officer' (Commander and above)
- Annual reporting obligations

Further Information

If you are intending on applying for a journalist information warrant, contact your s47E(d) for advice beforehand and the s47E(d)

If a journalist is the subject of the investigation and there is uncertainty about the need for a JIW contact AFP Legal to obtain guidance via email: s47E(d) or phone s47E(d)

s22(1)(a)(ii)

Pages 52 through 54 redacted for the following reasons:
---
s22(1)(a)(ii)

An enhanced proportionality test for data authorisations has been introduced as a result of the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* which came into effect on 13 October 2015.

Authorised officers are required to be 'satisfied on reasonable grounds' that any interference with the privacy of any person or persons that may result from the disclosure or use of the data is 'justifiable and proportionate', having regard to a range of factors.

An authorised officer **must** be aware of the following limitations prior to making an authorisation:

Journalist Information Warrants

Domestic requests

Section 180H(1) states:

An authorised officer **must not** make an authorisation under section 178, 178A (missing persons) or 180 that would authorise the disclosure of information or documents relating to a particular person if the authorised officer knows or reasonably believes that particular person to be:

- a person who is working in a professional capacity as a journalist, or
- an employer of such a person, **and**

a purpose of making the authorisation would be to identify another person is known or reasonably believed to be a source **unless** a JIW is in force.

Foreign Law Enforcement

There is **no provision** under Division 4A section 180A, 180B, 180C, 180D in relation to access or disclosure for **foreign law enforcement** for a JIW. The authorising officer **must not** make an authorisation that would authorise the disclosure of information or documents relating to a person who is working in a professional capacity as a journalist; or an employer of such a person; and a purpose of making the authorisation would be to identify a source.

Further information is available in the Better Practice Guide on procedures to obtain a journalist information warrant.

The below checklist has been developed to assist authorising officers in making the assessment that ensures ongoing legislative compliance can be demonstrated. If the authorising officer answers '**No**' to any of the below, the authorisation cannot be progressed.

Page 56 redacted for the following reason:
---
s47E(d)

AFP
AUSTRALIAN FEDERAL POLICE

Functional Governance
Better Practice Guide

Management of Access to Historical Telecommunications Information

Date of initial endorsement:	(select date first endorsed)
Date of last review:	(select date last reviewed)
Endorsed by:	Manager AOCC
Owner:	Manager AOCC
Contact:	AOCC s47E(d)
Identifier:	MAOCC006
IPS Status	(select option)

Disclosure and classification

This document is classified For Official Use Only and is intended for internal AFP use. Disclosing any content must comply with Commonwealth law and the AFP National Guideline on information management.

Compliance

This instrument is part of the AFP's professional standards framework. The AFP Commissioner's Order on Professional Standards (CO2) outlines the expectations for appointees to adhere to the requirements of the framework. Inappropriate departures from the provisions of this instrument may constitute a breach of AFP professional standards and be dealt with under Part V of the *Australian Federal Police Act 1979 (Cth)*.

This document is a functional governance instrument as defined under s.4 of the AFP Commissioner's Order on Governance (CO1).

Contents

Definitions

AFP appointee	Means a Deputy Commissioner, an AFP employee, special member, special protective service officer or other person engaged by the AFP to perform duties as an AFP employee or otherwise assisting the AFP as per s.4 of the *Australian Federal Police Act 1979* (Cth) (the AFP Act).
AFP member	Means a 'member of the AFP' as defined in s.4 of the AFP Act.
AFP Operations Co-ordination Centre (AOCC)	AOCC has 24/7 operational capacity and is responsible for actioning urgent after business hours IPND requests. Telecommunications Requests in matters where there is a 'Threat to Person's Life or Health' are actioned by the AOCC, under s.287 of the *Telecommunications Act 1997* on a 24/7 basis.
Authorisation form	Means the documentation authorising access to telecommunications information in accordance with the requirements of s.183 of the *Telecommunications (Interception & Access) Act 1979* (TIA Act).
Authorised Officer	(in relation to an enforcement agency) Is defined in s.5AB(1) of the *TIA Act* as the head or deputy head of an enforcement agency, persons acting in those positions, and individuals holding management positions within that agency who are authorised to perform this function.
Carrier	Means Australian telecommunications carriage service providers (CSP) and internet service providers (ISP) as defined in the *Telecommunications Act 1997* (Cth).
Data Retention	Means the continued storage of an organisation's data for compliance or business reasons. Carriers are required to comply with the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015* which came into effect on 13 October 2015.
Enforcement agency	Is defined in s.176A of the *TIA Act* and includes the Australian Federal Police (AFP).
s47E(d)	Is the AFP team responsible for processing requests for release of information from external agencies and businesses. s47E(d) s47E(d)
Historical telecommunications data	Means telecommunications information that is already in existence at the time of a request for access.
Prospective data	Means telecommunications information that is collected as it is created and forwarded to the agency in near real time as a result of a request for access.
Relevant staff member	Is defined in s. 5(1) of the *TIA Act* as the head of an agency, a deputy head of an agency or any employee, member of staff or officer of the enforcement agency. A relevant staff member of an enforcement agency is authorised to notify a carrier or carriage service provider of the making of an authorisation for the disclosure of historical or prospective telecommunications information. The AFP has determined that this notification role will be performed by the s47E(d) of the s47E(d) s47E(d) as detailed in this guideline.
Requesting Officer	Means an AFP appointee submitting a duly authorised request for telecommunications information.

Telecommunications information (data)	Is information about a communication or service. It does not include the content or substance of the communication. Telecommunications information is available in relation to all forms of communications, including both fixed and mobile telephony services and for internet-based applications including internet browsing and voice over internet telephony. s47E(d)
Telecommunications device	Means a device that is capable of being used for transmitting or receiving a communication over a telecommunications system.

Acronyms

AFP	Australian Federal Police
AGD	Attorney General's Department
AO	Authorised Officer
AOCC	AFP Operations Coordination Centre
s47E(d)	
CCR	Call Charge Records
CSP	Carriage Service Provider
s47E(d)	
GPRS	General Packet Radio Service
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
s47E(d)	
IP	Internet Protocol
IPND	Integrated Public Number Database

ISP	Internet Service Provider
JIW	Journalist Information Warrant
s47E(d)	
PROMIS	Police Real-Time Online Management Information System
RO	Requesting Officer
TIA Act	Telecommunications (Interception and Access) Act 1979
TID	Telecommunications Interception Division

Introduction

The objective of this Better Practice Guide is to clarify the role and services provided by the s47E(d) the role and responsibilities of AFP appointees when making requests for historical telecommunications information, and the procedures to be followed to obtain, use, record, disclose and report on such information.

Relevant documentation and information can be found on the AFP Hub, in the Investigator's Toolkit External Agencies Inquiries pages. The Investigator's toolkit is the primary reference point for all information about historical telecommunications information requests.

Key Legislation and notes

Telecommunications Act 1997

Telecommunications (Interception & Access) Act 1979 (TIA Act)

Privacy Act 1988.

Journalist Information Warrant (JIW):

The procedure for obtaining a Journalist information warrant is described in detail in the "Better Practice Guide for procedures to obtain a Journalist Information Warrant", and governed by the *Telecommunications (Interception & Access) Act 1979; Division 4C – Subdivisions A; B and C.*

Of particular note for requests for historical telecommunications information is s.180H of the TIA act (emphasis added):

> *180H*
>
> *(1) An authorised officer of an enforcement agency **must not** make an authorisation under section 178, 178A, 179 or 180 that would authorise the disclosure of information or documents relating to a particular person if:*
>
> > *(a) the authorised officer knows or reasonably believes that particular person to be:*
> >
> > > *(i) a person who is working in a professional capacity as a journalist; or*

(ii) an employer of such a person; and

(b) a purpose of making the authorisation would be to identify another person whom the authorised officer knows or reasonably believes to be a source; unless a journalist information warrant is in force, in relation to that particular person, under which authorised officers of the agency may make authorisations under that section.

Secondary disclosures:

The TIA Act allows secondary disclosure and use of the telecommunications information in certain circumstances. This allows enforcement agencies to pass on information to s7(1) where it is reasonably necessary for s7(1) to carry out its functions, or to another enforcement agency where it is necessary for the enforcement of the criminal law, a law imposing a pecuniary penalty or the protection of the public revenue.

Additional procedural requirements relating to authorisations:

The TIA Act imposes record keeping requirements on enforcement agencies. For historical telecommunications requests, these records are maintained by the s47E(d) s47E(d) and form the basis of an annual report to the Attorney-General on requests for access to telecommunications information. Any Journalist Information Warrant authorisation submitted tos47E(dfor action through the CSPs/ISPs are to be accompanied by an electronic copy (email) of the warrant which will be retained for audit purposes along with the authorisation itself.

s47E(d)

Requesting Officer (RO)

It is the Requesting Officer's (RO)'s responsibility to ensure that they are aware of the relevant legislation and procedures, that a legitimate requirement exists for the telecommunications information being sought, and that the subsequent request abides by the relevant legislation, procedures and guidelines.

The Checklist for Investigators, available through the AFP Hub Investigators' Toolkit is a handy tool to help guide ROs through the process.

s47E(d)

s47E(d)

s47E(d)

s47E(d)

Once satisfied of the need for information, the RO is to complete an authorisation form, available on the AFP Hub here Historical Telecommunications Request Authorisation Form. This authorisation process abides by requirements set out in legislation and issued by the Communications Access Coordinator, National Security Policy Branch, Department of Home Affairs. Members must only use the approved forms.

The electronic request authorisation form is 'dynamic' and responds to user input by making the relevant fields available depending on choices made. For some request types multiple entities can be nominated.

s47E(d)

s47E(d)

Once the RO has completed the request details, they should select the 'submit' button at the bottom of the form, which automatically forwards it by email to the Authorised Officer (AO) nominated on the form.

Authorisation form:

ROs should only use the 'submit request to authorising officer' button to process the form. Emailing or saving the form elsewhere will negate the auto-process and render the form invalid. See below for foreign criminal or international law requests which use a different form.

It is incumbent upon the RO to ensure any correspondence regarding a telecommunications request is uploaded to the log of their case and linked appropriately.

Authorised Officer (AO)

AO is defined to mean the head or deputy head of an enforcement agency, persons acting in those positions, and individuals holding positions within that agency who are authorised to perform this function. For the purpose of historical telecommunications requests, the Commissioner has determined that OIC, ACT Policing Intelligence (Band 8) and superintendents and above shall be authorised officers with the exception of JIW matters. Only Commanders can authorise JIW related checks.. Note that the authority is attached to

the position, not the individual, and therefore can be exercised by those officially holding or acting (with the appropriate delegation) in the relevant positions. *The delegated authority can only be exercised by a sworn member.*

A full list of Authorised Officers is managed centrally by AOCC | s47E(d)
Relevant delegations can be found at Delegations and Authorisations Collection, Telecommunications (interception and Access) Act 1979 - (ref. Part 4-1 of table)

AOs, in granting an authority, are to be satisfied that the request abides by handling, use and reporting procedures for historical telecommunications information, and complies with the requirements of the *TIA Act*, in particular ss. 178, 178A, 179, 180A, 180C and 180D.

s47E(d)

Foreign Law Enforcement Agency or International Requests and Authorisations

Please note that authorisations to access telecommunications data on behalf of a foreign law enforcement agency, the International Criminal Court or a war crimes tribunal are made on a different form to that used for ss.178, 178A and 179.

An authorisation under s180A applies if the information has not previously been disclosed by the carrier to the AFP. An authorisation under s180C applies if the AFP is making a secondary disclosure of information that has been previously obtained under ss178 or 179, with the exception of information obtained in relation to missing persons.

Information relating to the process for requests made under section 180A and 180C is available here: Process for the enforcement of the criminal law of a foreign country. (Please also note the Authorised Officer list within the document).

Disclosure to third parties

Please refer to the Investigators' Toolkit for the requirements for disclosing telecommunications information to third parties, here: Data retention - Third party information disclosure. The appropriate forms are Third party disclosure - Foreign LEA and Third party disclosure - Domestic LEA. Please note that third party disclosure authorisations are also subject to the requirements of the Data Retention legislation.

Steps to obtain historical telecommunications information:

Overview: historical telecommunications information request process

The various types of historical telecommunications requests may each have slightly different procedures to follow, which are outlined in detail on the Investigator's Toolkit/External Agencies Enquiries Hub pages. As previously stated, these pages are the primary resource to be consulted before addressing any query s47E(d) as they will contain the most up-to-date procedures and advice. s47E(d)

s47E(d)

s47E(d) . Please refer to the Investigator's

Toolkit site for the request forms and anything else you need to create a historical telecommunications information request.

In brief, the historical telecommunications information request process consists of determining the type of request/s required; establishing that the requested information can be lawfully obtained (and will not duplicate any information previously sought or obtained); completing the Historical Telecommunications Information Request Authorisation Form using the appropriate fields; and submitting the form for authorisation and forwarding to the CSP/ISP. Results from the CSP/ISP will be returned to s47E(d) the RO.

s37(2)(b), s47E(d)

s47E(d), s37(2)(b)

- **For ALL telecommunications information requests:**
  - Obtain authorisation via completing an Historical Telecommunications Information Request Authorisation Form which is a 'dynamic' document that responds to user input by making the relevant fields available depending on choices made.
  - For some request types multiple entities can be nominated. s47E(d)
    s47E(d)
  - Once the form is completed, submit it to the authorised officer, via the 'Submit Request to Authorising Officer' button at the end of the form.
  - When the authorised officer completes their input to authorise the request, they will select 'submit' on their part of the form, which will forward an email copy of the authorised request to the s47E(d)
  - s47E(d) in turn will submit the authorised request to the relevant CSP/ISP.
  - Once a result is received from the CSP/ISP, the s47E(d) will email a copy of the result to the RO.

    s47E(d)

  - This completes the information request process.

- **Request Priority and Contact Points - Historical Requests**

Rating	Request	Contact points
Routine	The information is required for an investigation/intelligence probe.	Processed during business hours. The contact point for **routine** requests is the s47E(d)
Urgent (excluding the below requests)	The circumstances are serious and urgent. A delayed response may affect the success of the operation.	Processed during business hours. The contact point for **urgent** requests is the s47E(d) (The s47E(d) should be notified of any urgent request).
Urgent - Telecommunications Interception Warrant Subscriber Check	The information is urgently required for a telecommunications intercept warrant in order to preserve evidence.	Processed during business hours. The contact point for **warrant** requests is the s47E(d) s47E(d) should be notified of any urgent request).

Life Threatening	The information is urgently required to prevent or lessen a serious and imminent threat to the life or health of a person. The requested response time is immediate. Follow link for further details.	The contact point for all **Life Threatening** checks is the AOCC Watchfloor. This applies 24 hours, 7 days a week. (The AOCC Watchfloor Supervisor should be contacted on extension s47E(d)

Cost of Requests/Financial Approval

The costs of Historical Telecommunication Information Requests are borne by the s47E(d) s47E(d) Team under a standing financial approval arrangement. However, it is still incumbent upon ROs to minimise costs to the AFP wherever possible. A detailed listing of the fees associated with requests can be found under the links for each CSP/ISP on the Investigator's Toolkit/External Agencies Enquiries Hub site. The costs associated with requests are updated regularly based on advice from the CSPs/ISPs – each has a separate schedule of fees. A handy 'pitfalls to avoid' page is also provided on the hub site. Any requests with a projected cost in excess of $500 will be queried by TL s47E(d) with a view to minimising the costs.

Record Keeping

Data Retention under the TIA Act 1979

The TIA Act stipulates the types of data to be retained, and for what period.

s47E(d) is required to periodically prepare a report for the Commonwealth Ombudsman detailing the types and numbers of authorisations sought (including authorisations for third party disclosure), and any breaches that may have occurred in the reporting period. 'Breaches' may include requests that are not in line with best practice or legislation, such as incorrect act and section, wrong request type, improperly authorised requests, results from CSPs/ISPs that do not conform to the request parameters (such as results outside specified dates), or incomplete request forms.

NOTE: Any Journalist Information Warrant authorisations submitted to s47E(d) for action through the CSPs/ISPs are to be accompanied by an electronic copy (email) of the warrant. s47E(d) will retain the email for audit purposes along with a copy of the authorisation itself.

Please note that representatives of the Commonwealth Ombudsman's office conduct regular inspections of AFP records and authorisations, and may wish to speak with individual AOs.

Privacy and Confidentiality

Unauthorised disclosure or mishandling of sensitive information is an integrity issue and will be dealt with accordingly. Breaches of confidentiality should be reported according to The AFP Commissioner's Order on Professional Standards (CO2).