A full list of all records to be kept by providers is available on the Investigator's Toolkit.

6.1 Life Threatening Matters

In the case of life threatening situations the following requests can be made through the AOCC Watchfloor or ACT Policing Operations:

- A trace on the location of a caller under s. 30 of the TIA Act
- Disclosure of information under s. 287 of the *Telecommunications Act 1997*
- Suspension of a carriage service under s. 315 of the *Telecommunications Act 1997*.

The AOCC Watchfloor Supervisor or ACT Police Duty Operations Manager should be contacted in the first instance on extension s47E(d) for the AOCC or extension s47E(d) for ACT Policing for life threatening situations. Further information can be found under Life Threatening Phone Calls on the AFP Hub.

6.2 Requests - Historical Telecommunications Data

An authorised officer must be satisfied that the disclosure of telecommunications data by the carrier is reasonably necessary for the enforcement of the criminal law (s. 178 of the TIA Act), for the purposes of finding a person who the AFP, or a Police Force of a State or Territory has been notified is missing (s. 178A of the TIA Act), or for the enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue (s. 179 of the TIA Act).

The Investigator's Toolkit outlines the process to obtain historical telecommunications data.

For each carriers cost schedule refer to the relevant service provider on Telecommunications in the Investigator's Toolkit.

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 points for **routine** checks are the s47E(d) in each office.
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 points for **urgent** requests are the s47E(d) in each office. (The s47E(d) should be notified of the urgent request on s47E(d)
Urgent -	The information is	Processed during business

Telecommunications Interception Warrant Subscriber Check	urgently required for a telecommunications intercept warrant in order to preserve evidence.	hours. The contact points for **warrant** requests are the s47E(d) in each office. (The s47E(d) should be notified of the urgent request on s47E(d)
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)

6.3 Requests - Prospective Telecommunications Data

An authorised officer must be satisfied on reasonable grounds of the criteria defined under s. 180 of the TIA Act that:

- The disclosure of prospective telecommunications data by the carrier is reasonably necessary for the investigation of a serious offence or an offence which attracts a term of imprisonment of at least 3 years; and
- Any interference with the privacy of any person or persons resulting from the disclosure or use of the data is justifiable and proportionate in the circumstances, having regard to a range of factors. This may include, for example, an assessment of the value of the information sought compared to the privacy of the user or users of the telecommunications service in question.

The authorised officer should ensure these tests are applied correctly and be aware the request could become invalid in any future legal proceedings if it can be shown that the privacy considerations obviously outweighed the value of any potential data sought.

The Investigator's Toolkit outlines the procedures to obtain prospective telecommunications data.

For carrier connection fees please see Telecommunication carrier fees on Telecommunications Intercepts and Stored Communications on the Investigator's Toolkit.

The Investigator's Toolkit contains the BPG Management of Access to Prospective Telecommunications Data

6.4 Revocations - Prospective Telecommunications Data

Revocations are only relevant to the access of prospective telecommunications data.

An authorised officer must revoke the authorisation if they are satisfied the disclosure of the telecommunications data is no longer required.

s47E(d) will cease the authorisation in the AFP interception systems prior to serving the Authorised revocation forms on the carrier to ensure that there is no telecommunications data received after the carrier receives the revocation, which would constitute an unauthorised disclosure.

Revocation forms can be found on the Telecommunications Intercepts and Stored Communications on the Investigator's Toolkit.

The Investigator's Toolkit contains the BPG Management of Access to Prospective Telecommunications Data

6.5 Disclosure to a Foreign Country

Disclosure from the Carrier to the AFP

In order to allow foreign law enforcement agencies (LEA) access to existing historical and prospective telecommunications data for the enforcement of a criminal law of a foreign country, the AFP must follow a two-step process for the two different authorisations.

The BPG Management of Access to Historical Telecommunication Information outlines the steps for historical telecommunications data utilising section 180A of the TIA Act.

The BPG Management of Access to Prospective Telecommunication Data outlines the steps for prospective telecommunications data utilising section 180B of the TIA Act.
A mutual assistance request must exist before a 180B (2) authorisation can be made. AGD will make an authorisation under 15D of the Mutual Assistance Act.

A 180B (2) authorisation can only be extended once, making the maximum duration 42 days.

Disclosure from the AFP to a foreign LEA

A requesting officer must not disclose telecommunications data to a foreign law enforcement agency unless the disclosure is subject to the following conditions:

- The information/data will only be used for the purposes for which the foreign LEA requested it

- Any data from a 180B authorisation will be destroyed when it is no longer required for those purposes
- Any other condition imposed by the Attorney-General Department (AGD).

An authorised officer can only make one 180B (8) authorisation a day, ensuring that prospective telecommunications data is reviewed by the AFP before further disclosure to the foreign LEA.

Section 180C of the TIA Act allows the AFP to disclose to a foreign LEA telecommunications data that has previously been obtained by the AFP under Division 4 of the TIA Act, with the exception of data previously obtained to locate a missing person.

Foreign law enforcement disclosure forms can be found on Data Retention on the Investigator's Toolkit.

s22(1)(a)(ii)

6.7 Privacy Considerations

Authorisations for telecommunications data involve an impact on an individual's privacy. Section 180F of the TIA Act outlines that authorising officers 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 of the data is justifiable and proportionate, having regard to the following matters:

- The gravity of the conduct being investigated, including the seriousness of any offence or penalty in relation to which the information is sought
- The reason why the disclosure is proposed to be authorised
- The likely relevance and usefulness of the information to the investigation.

Further information can be found on the AGD Information Sheet 19 - New Privacy Test.

6.8 Journalist Information Warrants (JIW)

A JIW is required if an investigator intends to obtain an authorisation to access telecommunications data relating to a journalist, and a purpose in doing so is to identify a journalist's source..

JIW forms can be found in the Investigator's Toolkit page for Data Retention.

Your s47E(d) should be contacted prior to requesting a JIW, as they will put in contact with the lead s47E(d) for all JIW related activities nationally. Engagement with AFP Legal is required for all JIWs.

The BPG Procedures to obtain a Journalist Information Warrant is available on the Investigator's Toolkit and provides further detail.

6.9 Use and Disclosure

S. 180D of the TIA Act allows the telecommunications data obtained on behalf of a foreign LEA to be used by the AFP or further disclosed to an enforcement agency (as defined under s. 176A of the TIA Act), where the disclosure is reasonably necessary for the enforcement of the criminal law, a law imposing a pecuniary penalty, or the protection of the public revenue, or if a disclosure is made to s7(1) as is reasonably necessary for the performance of its functions.

Sections 181B and 182 of the TIA Act set out the circumstances in which enforcement agencies are able to use and disclose telecommunications data as a result of an authorisation.

Pursuant to s. 182(2) an AFP appointee may, for a permitted purpose in relation to AFP, disclose telecommunications data to another AFP appointee.

S. 182(2A) of the TIA Act allows the disclosure of telecommunications data when the disclosure is reasonably necessary for the purpose of finding a missing person.

For further information please contact the s47E(d) team.

6.10 Authorisation Forms

S. 183 of the TIA Act provides that all authorisations, notifications and revocations for access to telecommunications data must be in written or electronic form and comply with such requirements as determined by the Communications Access Coordinator. In effect, this means that all requests for access to telecommunications data must be in the prescribed format provided on the AFP Hub - any other form will not be valid. All forms are located on the Investigators Toolkit.

6.11 Notification to Carrier

In line with sections 184(3) and (4) of the TIA Act, a member of the s47E(d) (as the *relevant staff member* of the AFP) must notify the telecommunications service provider or internet service provider from whom the disclosure is sought, or from whom a revocation of authorisation is sought.

s22(1)(a)(ii)

s22(1)(a)(ii)

6.13 Reporting

The AFP is required to report annually to the Department of Home Affairs regarding its access to telecommunications data.

The AFP's report must include statistics on the number of authorisations made during the previous financial year and any other matter requested by the Minister in relation to those authorisations

The AFP's report must also include information on the offence types, the type and length of retained data sought and the name of each foreign country a disclosure was made to.

The capture and maintenance of the required statistics will be completed by s47E(d) and TID, with relevant statistics provided to the Department of Home Affairs as required.

Section 185 of the TIA Act stipulates that all authorisations must be retained by the requesting agency for a period of no less than 3 years. Currently, there are no destruction requirements in relation to authorisations or the data accessed as a result of an authorisation.

6.13 Commonwealth Ombudsman oversight and reporting

Pursuant to the TIA Act, the Commonwealth Ombudsman must inspect the records of the AFP to determine the extent of compliance with the TIA Act and report annually on:

- Historical Telecommunications Information requests
- Prospective Telecommunications Data requests

7. Roles and Responsibilities

7.1 Requesting Officer Responsibilities

Requesting officers must:

- Comply with legislation and AFP procedures outlined in the Investigator's Toolkit when producing an authorisation form for consideration by the authorising officer
- Maintain appropriate case management records in relation to received telecommunications data
- Ensure relevant team members are briefed on handling, use and reporting procedures for telecommunications data.

7.2 Authorised Officer Responsibilities

In addition to the Commissioner and Deputy Commissioners the Commissioner has authorised that AFP members occupying, or holding the ranks of the, the following management positions, be authorised officers:

- Assistant Commissioner
- Commander
- Superintendent
- Officer in Charge, ACT Policing Intelligence.

It is important to note that only Commanders and above make authorisations in relation to JIWs.

Instruments of Authorisation s. 5AB(1) and s. 5AB(1A) of the TIA Act, (Refer Delegations and Authorisations Collection)

Note this authority is attached to the position, not the individual, and therefore can be exercised by those officially holding or acting in the above-mentioned sworn positions. Authorised officers must be satisfied on reasonable grounds that any interference with the privacy of any person or persons that may result from the application, disclosure or use of the telecommunications data is justifiable and proportionate to a range of matters set out in section 180F of the TIA Act..

For detailed information on the application and authorisation process refer to the 'Historical Telecommunications Requests' and 'Considerations for Authorising Officers' documents located within the Data Retention page of the Investigator's Toolkit.

7.3 s47E(d) Responsibilities

s47E(d) will:

- Provide advice to requesting officers in the preparation of applications for authorisations to access historical telecommunications data
- Process all requests for access to historical telecommunications data
- Maintain records of authorisations made
- Perform the role of *relevant staff member* in relation to notifying carriers and carriage service providers about the authorisation of a request for historical telecommunications data
- Return results to the requesting officer
- Keep records in relation to the telecommunication requests and report to the Minister and Department of Home Affairs as required
- Facilitate inspections by the Commonwealth Ombudsman

7.4 AFP Operations Coordination Centre (AOCC) Responsibilities

AOCC Watchfloor will:

- Process all historical requests marked as Life Threatening
- Perform the role of *relevant staff member* in relation to notifying carriers and carriage service providers about the authorisation of a request for historical telecommunications data in life threatening situations
- Assist relevant requesting officers in the preparation of material in relation to the above applications
- Notify s47E(d) if a request under Division 4 of the TIA Act is processed outside of business hours.

7.5 s47E(d) Responsibilities

s47E(d) will:

- Provide advice to requesting officers in the preparation of material in relation to applications for authorisations to access prospective telecommunications data

- Provide advice to requesting officers in the preparation of material in relation to revocations of authorisations for access to prospective telecommunications data
- Where the request relates to Telecommunications Intercept Warrants, liaise with s47E(d) to determine capacity for handling the request, and where appropriate forward the request to s47E(d) for appropriate processing.
- Vet the relevant documents and attend s47E(d) Committees for all Telecommunications Interception Warrants

7.6 s47E(d) Responsibilities

s47E(d) will:

- Process all requests for access to prospective s47E(d) s47G(1) s47G(1) data
- Maintain records of authorisations for access to prospective s47E(d) s47G(1) s47G(1) data, and any related revocations
- Perform the role of *relevant staff member* in relation to notifying carriers and carriage service providers about the authorisation of a request for or revocation of disclosure of prospective telecommunications data.
- Facilitate inspections by the Commonwealth Ombudsman
- Provide an initial helpdesk role for the administration of AFP interception systems.

8. Further Advice

Queries about the content of this guideline should be referred to:
On access to historical data: s47E(d) hub page or s47E(d)
On access to prospective data: s47E(d) page or s47E(d)
On legal issues: AFP Legal hub page or Legal-Advisor or the Legal Hotline extension s47E(d)

References

Legislation

- *Australian Federal Police Act 1979* (Cth)
- *Telecommunications Act 1997* (Cth)
- *Telecommunications (Interception and Access) Act 1979* (Cth)
- *Privacy Act 1988* (Cth)
- *Mutual Assistance in Criminal Matters Act 1987* (Cth)

AFP governance

- AFP National Guideline on information management
- AFP National Guideline on telecommunications and stored communications

Other sources

- Data Retention – AFP HUB
- s47E(d) Telecommunications - AFP Hub Page.

s22(1)(a)(ii)

Subject: FW: Authorised Officer training mandatory [DLM=For-Official-Use-Only]

From: Stewart, DavidJ
Sent: Friday, 17 November 2017 4:20 PM
To: s22(1)(a)(ii)
Subject: Authorised Officer training mandatory [DLM=For-Official-Use-Only]

For-Official-Use-Only

All AFP SES/EL Members

The iAspire online – *Authorised Officer training* - is now available.

The eLearning training package has been developed by TID in conjunction with L&D online-learning, AFP Legal and the Commonwealth Ombudsman's Office. The package provides all AFP Authorised Officers with the key points and considerations necessary to perform the duties of an Authorised Officer under the *Crimes Act 1914*, the *Telecommunications (Interception and Access) Act 1979*, and the *Surveillance Devices Act 2004*; and to ensure Authorising Officers:

- understand the powers and statutory obligations under the legislative regimes;
- be aware of the potential adverse consequences of authorising an investigative power incorrectly; and
- know where to find assistance and resources to meet your obligations on the Investigators Toolkit.

Please note: the Commissioner has directed that this training course is a mandatory requirement for all EL and SES members before they can exercise their delegation as an Authorised Officer according to the relevant legislation.

You will be expected to complete the training course by 15 December 2017

The link below can be used to access the training directly.

http://afp.pulselms.com/FClient/bin/PulseClient.aspx?dlink=1106

Further information about TID activities and updated metadata processes, including amended forms, data authorisation templates and training and reference material, and a new Better Practice Guide on Procedures to obtain a Journalist Information Warrant is available on the Investigators Toolkit.

All investigators and Authorised Officers are expected to familiarise themselves with contemporary content pertaining to data retention and Journalist Information Warrants.

The training should take about 60 minutes to complete and has 16 questions embedded which you are require to obtain 80% correct to successfully complete the training.

MAOCC will be undertaking weekly audits of the level of completion of the training. If you do not complete the package within the allocated 4 week period you will not be permitted to use your delegation as an Authorised Officer pursuant to the Crimes Act 1914, the Telecommunications (Interception and Access) Act 1979, and the Surveillance Devices Act 2004 until completed.

Regards,

DAVID STEWART
ASSISTANT COMMISSIONER
SUPPORT CAPABILITY
Tel + s22(1)(a)(ii)
www.afp.gov.au

AFP
AUSTRALIAN FEDERAL POLICE

POLICING FOR
A SAFER AUSTRALIA

For-Official-Use-Only

Welcom s22(1)(a)(ii)

AFP AUSTRALIAN FEDERAL POLICE Investigator's Toolkit

Back to The Hub

AFP Hub > Operational info and resources > Investigator's Toolkit > Special projects > AFP Authorised Officers access to telecommunications metadata

AFP Authorised Officers access to telecommunications metadata

Overview

This page will cover:

- TIA Act telecommunications data retention regime
- information available from the carriers
- authorisation types
- privacy considerations
- Journalist Information Warrants
- obligations of an AFP Authorised Officer (AO)
- common errors identified
- oversight by Commonwealth Ombudsman
- relevant areas.

Regime

- limited the range of agencies that are able to access telecommunications data and stored communications
- established a journalist information warrants (JIW) regime
- created the Public Interest Advocate role to provide further oversight in relation to JIWs
- requires record-keeping on the use of, and access to telecommunications data
- enables the Commonwealth Ombudsman to assess agency compliance
- required carriers to maintain data records.

Data set

Carriers and ISPs retain these six kinds of information for two years (unless exempted)

1. subscriber and account information

2. source of a communication
3. destination of a communication (not ISPs)
4. date, time and duration of communication
5. type of communication (MMS, SMS, IP address information, voice mail, email, etc.)
6. location of device.

Location identifies the closest relay tower/s where the service/equipment was being used.

Authorisations - Domestic - division 4

An AO **must not** make an authorisation under s178, s178A, s179 or s180 if the person subject of the disclosure is a journalist or an employer of such and a purpose for making the request is to identify a possible source, without obtaining JIW.

Only a **Commander and above** may make an authorisation where a JIW is required, and has been obtained.

An AO under s5AB(1) can issue

- s178 - enforcement of the criminal law
- s178A - locate missing persons
- s179 – protection of public revenue/enforcement of criminal law/law imposing pecuniary penalty, which authorises disclosure of historical (existing) information
- Subscriber checks, IPND, CCRs
- s180 – State, Territory or Commonwealth offence sentence 3years or more authorises the disclosure of prospective information for a period of effect of 45days

s47E(d), s47G(1)

Authorisations - Foreign division 4A

There is no provision under section 180A, 180B, 180C,180D in relation to access or disclosure for a foreign law enforcement agency (FLEA) for a Journalist Information Warrant. The AO 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 where a purpose of making the authorisation would be to identify a source.

There is also no provision to disclose information to a FLEA under 180C, if

that information was obtained under an authorisation made under section 178A (missing persons).

An AO authorised under s5AB(1A) for the purpose of enforcement of the criminal law of a foreign country with a minimum sentence of 3 years or involves an act or omission that if it had occurred in Australia would have constituted a serious offence (minimum sentence 7years) can issue a:

- s180A – access to historical (existing) information
- s180B – access to prospective information.
- an MAR must be in place prior to the s180B authorisation being made.
- s180C – secondary disclosure historical (existing) information resulting from a s178 or s179, s180 domestic authorisation or
- s180D – authorisation to disclose information received under Division 4 to the organisation or a law enforcement agency and/or the use by the AFP for the enforcement of the criminal law or enforcement of the law imposing a pecuniary penalty.

Privacy considerations

Why privacy considerations are paramount

The Act was designed to protect the privacy of telecommunications. The data retention amendment added extra protection, including the JIW regime. The basis of the amendment being the fundamental right to privacy, freedom of expression including the freedom to seek, receive and impart information and ideas of all kinds.
Basically the freedom of the press by ensuring the correct protection for sources.

What does this mean to an AO ?

A precis of 180F of the Act states that before an AO makes an authorisation under Division 4 or 4A

the AO must be satisfied on reasonable grounds, from information provided by the applicant that any interference with the privacy of any person or persons that may result from the disclosure or use of the information/documents specified is justifiable and proportionate having regard to

- the seriousness of the offence, including any pecuniary penalty and/or protection of public revenue in relation to which the authorisation is sought
- whether the authorisation is sought for the purpose of finding a missing person
- the likely relevance and usefulness of the information or documents

- the reason/s why the disclosure or use concerned is proposed to be authorised.

Note: An authorisation cannot be made under Division 4A, for the disclosure of

- information relating to a journalist (or their employer), where a purpose is to identify a source, because you can't get a JIW; or
- information obtained under an authorisation made under section 178A (missing persons) (s. 180C(1)).

Journalist Information Warrants

The data amendment regime added the extra privacy provisions to prevent access to historic or prospective data if the person subject of the disclosure is a journalist or an employer of such and a purpose for making the request is to identify a possible source without a JIW.

Note: Only a Commander and above can approve the commencement of a JIW process and authorise any authorisations required under it.

The role of the Public Interest Advocate (PIA)

PIAs are appointed by the Prime Minister to review JIW applications and provide submissions to the issuing authorities in relation to a decision to issue, or refuse to issue a JIW and/or decisions about conditions or restrictions (if any), that are to be specified in the warrant.

Other Requirements

The Commissioner must, as soon as practicable, provide to the Minister and the Ombudsman a

- copy of the journalist information warrant and
- any authorisations made under the warrant.

The Commissioner may revoke a journalist warrant 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, under 180W(2), may delegate this power to a 'certifying officer' (Commander and above).

Refer to the BPG on procedures to obtain a Journalist Information Warrant.

What if the journalist is being investigated for a serious criminal offence and a purpose of the authorisation is not to identify a source?

The Act defines the requirements of obtaining a JIW as related to the

identification of a source. Where there are any concerns in relation to obtaining the data of a journalist (or their employer), AFP Legal should always be consulted prior to the making of any authorisations.

Only a Commander and above can authorise authorisations under a JIW.

Obligations of an AO

Under section 180F of the TIA Act, before making an authorisation under Division 4 or 4A, the AO must be satisfied on reasonable grounds that any interference of the privacy of any person/s is justifiable and proportionate to the gravity of the conduct being investigated, as well as other matters.

This is achieved by

- applicants providing sufficient information in the application or via other briefing methods to the AO to enable the assessments to be made to grant the authorisation
- AO needs to be able to articulate their reasoning against the criteria under section 180F if their decision is tested.

Templates for requests and authorisations are located on the Investigators Toolkit.

Obligations of an AO recap

- authorisations must be issued before any disclosure of information
- consider whether a JIW is required
- authorisation cannot be made under Division 4A (FLEA), in circumstances where a JIW would be required, or for disclosure of 178A (missing persons) information
- authorisation for s180B (FLEA) prospective information must have an MAR in place first
- authorisations must use the templates on the Investigators Toolkit
- authorisations must only be issued when the matters outlined in s180F are satisfied
- records must be kept to demonstrate that authorisations were properly made.

Processing areas

Historic authorisation request forms is located on the Data Retention page and are processed by s47E(d)

- forms are completed electronically and are automatically emailed to the AO
- AO considers the request and approves or rejects, if approved the form is emailed to s47E(d)

- results are emailed to the requesting officer when available.

S180(2) Prospective authorisation request form is located on the Investigators Toolkit and are processed by s47E(d) s47E(d)

- form is completed either manually or electronically and is either presented or emailed to the AO
- AO considers the request and approves or rejects, if approved the authorisation is emailed to s47E(d) s47E(d)

Common errors

Common errors identified in the s180(2) prospective data authorisations include

- no offence category selected
- incomplete legislation listed
- correct offence with incorrect legislation
- AO signing but not dating manual copies.

As previously mentioned the AO must have the ability to articulate the reason for authorising the request if tested, this includes the assurance of the content of the authorisation. TID maintains a self disclosure register for the purpose of Commonwealth Ombudsman inspections and provides feedback to both investigators and applicants if errors are identified.

Record keeping requirements

s186A: Obligation to keep records in relation to Authorisations:

- each authorisation
- if authorisation/revocation was properly made
- use and disclosure of information obtained under authorisation
- evidentiary certificates.

All authorisations, results and associated documentation including the self disclosures registers are stored and maintained centrally within TID for reporting purposes to the Commonwealth Ombudsman.

Further information

- Investigators Toolkit
- Better Practice Guides

- s47E(d)
-

Last modified: 6/10/2017 9:23 | **Review due:** 5/10/2018 | **Author:** s47E(d)

Welcome s22(1)(a)(ii)

AFP AUSTRALIAN FEDERAL POLICE Investigator's Toolkit

Back to The Hub

AFP Hub > Operational info and resources > Investigator's Toolkit > Special projects > Data Requests - Information for Requesting and Authorising Officers

Data Requests - Information for Requesting and Authorising Officers

Section 180(4) and 180H(1) of the Telecommunications (Interception and Access) Act 1979 (the Act) state:

The authorised officer (AO) **must not** make the authorisation unless he or she is satisfied that the disclosure is reasonable 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.**

An AO **must not make an authorisation under section 178, 178A, 179 or 180 of the Act** that would authorise the disclosure of information or document relating to a particular person if:

a. the AO 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 the authorisation would be to identify a another person whom the AO knows or reasonably believes to be a source.**

Unless a **journalist information warrant (JIW) is in force**, in relation to that particular person.

Note: *There is **no provision** under Division 4A section 180A, 180B, 180C, 180D in relation to access or disclosure for a foreign law enforcement agency for a JIW.*

For further information in relation to circumstances and procedures in relation to journalist sources review the Better Practice Guide on the Procedure to obtain a Journalist Information Warrant.

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.

The application

The requesting officer is required to:

s47E(d)

- provide information linking the POI to the offence for example, s47E(d), s37(2)(b)

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

- information supplied must be contemporaneous

s47E(d)

- prospective data requests can be authorised only to investigate offences punishable by imprisonment of at least three years not just to gather intelligence.

s47E(d)

- ensure the correct offence section and legislation is included on the Authority or it will be rejected

The Authorisation

The AOs are required to ensure:

- A s180(2) **is not granted** if it relates to the circumstances delineated under section 180H without a JIW and/or any uncertainties in relation to circumstances surrounding an investigation into a journalist and/or employer have been addressed with AFP Legal.
- the legislation section and Act is complete and correct
- after reviewing the privacy considerations the information provided by the applicant sustains the decision to grant the Authority
- the period of effect requested is within the legislated 45 day time frame

- adequate information is available to articulate the decision making process, if required by the Commonwealth Ombudsman during inspection

Guidance on new privacy consideration

Last modified: 19/05/2017 15:58 | **Review due:** 12/10/2016 | **Author:** "> s47E(d)

AFP AUSTRALIAN FEDERAL POLICE

Process for the enforcement of a criminal law of a foreign country

Sections 180A and 180C allow Foreign Law Enforcement Agencies (FLEA) access to existing information or documents (historic telecommunications data) for the enforcement of a criminal law of a foreign country.

Note: There is **no provision** under section 180A, 180B, 180C,180D in relation to access or disclosure for a foreign law enforcement agency for a Journalist Information Warrant. 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.

180A – Authorisation for access to existing information or documents for enforcement of the criminal law of a foreign country

180A applies if the information has not previously been disclosed by the carrier to the AFP.

This process entails:

- The AFP applies for the information on behalf of the FLEA;
- The telecommunications carrier then provides the information to the AFP; and
- The AFP (subject to any sanitisation) provides the information to the FLEA.

Direction for Investigators

180A(2) - Authorising disclosure from carrier to the AFP

To be used for the disclosure of historical telecommunications data from an Australian telecommunications carrier to the AFP for the enforcement of a criminal law of a foreign country. The request is conducted by the AFP on behalf of the FLEA. The carrier provides the information to the AFP.

1. Complete the 180A(2) form and submit to an approver listed in the 5AB(1A) authorised officers list.
2. Scan and send the approved form via PROMIS task to s47E(d) s47E(d) to action.
3. Upon receipt of results, ensure they are uploaded to the relevant PROMIS case.

180A(4) - Authorising disclosure from the AFP to FLEA

To be used for the disclosure of historical telecommunications data from the AFP to the FLEA for the enforcement of a criminal law of a foreign country.

1. Complete the form and submit to an approver listed in the 5AB(1A) authorised officers list.
2. Send approved form via PROMIS task to s47E(d) for information.

180C – Secondary disclosure for the enforcement of the criminal law of a foreign country

Allows the disclosure of information that has previously been obtained under Division 4 – Part 4-1 (sections 178, 179 & 180, with the exception of 178A – missing persons).

This process entails:

- The AFP (subject to any sanitisation) provides information previously obtained under an existing s178, 179 or 180 authorisation to the FLEA (excludes s178A).

Direction for Investigators

180C - Authorising disclosure from the AFP to FLEA

To be used for the disclosure of previously obtained historical telecommunications data from the AFP to the FLEA for the enforcement of a criminal law of a foreign country.

1. Complete the form and submit to an approver listed in the 5AB(1A) authorised officers list.
2. Send approved form via PROMIS task to s47E(d) for information.

Pages 115 through 145 redacted for the following reasons:
---
s47E(d)