AFP National Guideline on access to telecommunications data

1. Disclosure and compliance

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.

This instrument is part of the AFP's professional standards framework. The AFP Commissioner's Order on Professional Standards (CO2) outlines the conduct expected of AFP appointees. 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).

2. Guideline authority

This guideline was issued by Deputy Commissioner Capability using power under s. 37(1) of the *Australian Federal Police Act 1979* (Cth) as delegated by the Commissioner under s. 69C of the Act.

3. Introduction

This guideline outlines the obligations for AFP appointees when utilising powers under the *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA Act) to access telecommunications data.

4. Legislation

The role of the TIA Act is to protect the privacy of individuals who use the Australian telecommunications system and specify the circumstances in which it is lawful to obtain, use and disclose telecommunications data.

Under the TIA Act, carriers and carriage service providers must keep the following kinds of historic telecommunications data, the:

- identifying details of the subscriber of a service, relevant account information, and other identifying details relating to the relevant service
- source of the communication
- destination of a communication
- date, time and duration of a communication, or of its connection to a relevant service
- type of a communication and relevant service used in connection with a communication
- location of equipment or a line used in connection with a communication.

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

s47E(d)

4.1 Life-threatening situations

s47E(d)

4.2 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).

s47E(d)

s47E(d)

s47E(d)

4.3 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 both:

- 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
- 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.

s47E(d)

4.4 Revocations - prospective telecommunications data

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

s47E(d)

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

s47E(d)

4.5 Disclosure to a foreign country

Disclosure from the carrier to the AFP

In order to allow foreign law enforcement agencies (FLEAs) access to existing historical and prospective telecommunications data for the enforcement of a criminal law of a foreign country,

s47E(d)

s47E(d)

A mutual assistance request must exist before a 180B (2) authorisation can be made. The Attorney-General's Department (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 FLEA

A requesting officer must not disclose telecommunications data to a FLEA unless the disclosure is subject to the following conditions:

- The information/data will only be used for the purposes for which the FLEA 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 AGD.

s47E(d)

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 FLEA.

Section 180C of the TIA Act allows the AFP to disclose to a FLEA 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.

s47E(d)

4.6 International Criminal Court (ICC) or a War Crimes Tribunal

The same two-step process may also be followed to allow the ICC or a War Crimes Tribunal access to existing historical or prospective telecommunications data for the purpose an investigation or prosecution of a crime within the jurisdiction of the ICC or a War Crimes Tribunal offence.

4.7 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:

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

s47E(d)

4.8 Journalist information warrants (JIWs)

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.

4.9 Use and disclosure

s47E(d)

Section 180D of the TIA Act allows the telecommunications data obtained on behalf of a FLEA 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 the organisation 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 business, disclose telecommunications data to another AFP appointee.

Section 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.

s47E(d)

4.10 Authorisation forms

Section 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 Investigator's Toolkit.

s47E(d)

4.12 Evidentiary certificates/packages

Evidentiary packages

Section 185C of the TIA Act permits a certifying officer of the AFP (as defined under s. 5AC of the TIA Act –

s47E(d)

s47E(d)

s47E(d)

Evidentiary certificates

Section 185A of the TIA Act allows an employee of a service provider/carrier to issue a written certificate in order to enable the disclosure of information or a document covered by an authorisation.

s47E(d)

Court statements

s47E(d)

4.13 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.

s47E(d)

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.

4.14 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.

5. Roles and responsibilities

s47E(d)

s47E(d)

s47E(d)

7. 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

- s47E(d)

8. Shortened forms

AGD	Attorney-General's Department
AFP	Australian Federal Police
AOCC	AFP Operations Coordination Centre

s47E(d)

s47E(d)	
FLEA	Foreign law enforcement agency
s47E(d)	
JIW	Journalist information warrant
s47E(d)	
TIA Act	*Telecommunications (Interception & Access) Act 1979*
s47E(d)	

9. Definitions

AFP appointee means a Deputy Commissioner, an AFP employee, special member or special protective service officer and includes a person:

- engaged overseas under s. 69A of the *Australian Federal Police Act 1979* (Cth) (AFP Act) to perform duties as an AFP employee
- seconded to the AFP under s. 69D of the AFP Act
- engaged under s. 35 of the AFP Act as a consultant or contractor to perform services for the AFP and determined under s. 35(2) of the AFP Act to be an AFP appointee.

(See s. 4 of the AFP Act.)

Authorisation form means the documentation authorising access to telecommunications data in accordance with the requirements of s. 183 of the 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. s47E(d)

s47E(d)

Carrier means any Australian telecommunications carriage service providers and internet service providers as defined in the *Telecommunications Act 1997* (Cth).

Communications Access Coordinator is established by s. 6R of the TIA Act as the first point of contact for both the telecommunications industry and agencies in relation to access to telecommunications data, and replaces the previous position of Agency Coordinator. They sit within the Department of Home Affairs.

Enforcement agency is defined in s.176A of the TIA Act and includes the Australian Federal Police (AFP).

s47E(d)

Foreign law enforcement agency is defined in s. 5 of the TIA Act.

Historical telecommunications data means telecommunications data that is already in existence at the time of the request for access to that data.

Prospective data means telecommunications data that is collected as it is created and forwarded to the agency in near real time as a result of the request for access to that data.

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 data. s47E(d)

s47E(d)

Telecommunications data is information about a communication (i.e. the who, when, where and how). It does not include the content or substance of the communication. Telecommunications data 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.

For telephone-based communications, telecommunications data includes:

- subscriber, purchase and billing information
- call charge records. s47E(d)

s47E(d)

In relation to internet-based applications, telecommunications data includes:

- subscriber, account, purchase and billing information
- the internet protocol (IP) address used for the session as well as the start and finish time of each session

s47E(d)