National Guideline on Access to Telecommunications Data

Disclosure and compliance

This document is classified **PROTECTED** and is intended for internal AFP use.

Disclosing any content must comply with Commonwealth law and the AFP National Guideline on disclosure of information.

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).

Acronyms

AFP	Australian Federal Police
AOCC	AFP Operations Coordination Centre
s7(2A)	
CAC	Communications Access Coordinator
CAD	Call Associated Data
CFI	Commissioner's Financial Instruction
s37(2)(b)	
PROMIS	Police Real-time Online Information System
SEDNode	Secure Electronic Disclosures Node
s37(2)(b)	
TIA Act	*Telecommunications (Interception & Access) Act 1979*
s37(2)(b)	

Definitions

Authorisation form - refers to the documentation authorising disclosure of telecommunications data in line 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 the TIA Act (s. 5AB) as 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.

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 information, and replaces the previous position of Agency Coordinator.

Criminal law-enforcement agency - is defined in the TIA Act to mean a body covered by any of the paragraphs (a) to (k) of the definition of 'enforcement agency' in subsection 5(1) of the TIA Act. This definition is required as only criminal law-enforcement agencies will be able to access telecommunications data on a prospective basis.

Enforcement agency - is defined in s.282(10) of the *TIA Act* and includes the AFP.

External Enquiries Team - is the AFP team or person responsible for processing requests for release of information from external agencies and businesses. External Enquiries teams are located in most of the larger AFP offices.

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 the TIA Act (subsection 5(1)) 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. s37(2)(b)

s37(2)(b)

Telecommunications data - is information about a telecommunication, but 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 information
- The telephone numbers of the parties involved
- The time of the call and its duration.

In relation to internet-based applications, telecommunications data includes the Internet Protocol (IP) address used for the session and the start and finish time of each session.

Authority to Create the Guideline

This guideline was created by the National Manager Forensic and Technical 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.

Introduction

This National Guideline sets out the AFP procedures to access telecommunications data under the new system established by the *Telecommunications (Interception & Access) Amendment Act 2007*.

Key Legislative Changes

The provisions of the *Telecommunications (Interception & Access) Amendment Act 2007* which commenced on 1 November 2007, amend the *Telecommunications (Interception & Access) Act 1979* (TIA Act) and the *Telecommunications Act 1997* by transferring the provisions of the *Telecommunications Act 1997* (the Telecommunications Act) that governed access to telecommunications data to the TIA Act.

While these provisions remain fundamentally unchanged, the key differences between the old system and this new approach which this National Guideline provides guidance on are:

- **Prospective data**: The new legislation makes a distinction between access to historical telecommunications data (data that is already in existence at the time of the request) and prospective data (data that is collected as it is created and forwarded to the agency in near real time). s7(2A)

s7(2A)

- **Secondary disclosures**: The TIA Act allows secondary disclosure and use of the telecommunications data in certain circumstances. s7(2A)

s7(2A)

s7(2A) where it is necessary for the enforcement of the criminal law, a law imposing a pecuniary penalty or the protection of the public revenue.
- **Procedural requirements relating to authorisations**: New record keeping requirements are placed on enforcement agencies, which will be the basis of an annual report to the Attorney-General on the number of their requests for access to telecommunications data.

s37(2)(b)

s37(2)(b)

Authorised Officer responsibilities

Authorised Officer 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. The Commissioner has determined that selected positions/ranks of coordinators/superintendents and above shall be authorised. Note that 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 positions.

s37(2)(b)

s37(2)(b)

s37(2)(b)

Applications for Authorisations

Section 183 of the*Telecommunications (Interception & Access) Act 1979* (TIA Act) provides that an authorisation and notification of an authorisation by the Australian Security Intelligence Organisation or an enforcement agency must comply with any requirements determined by the Communications Access Coordinator (CAC) and be in either written or electronic form. s37(2)(b)

s37(2)(b)

Access to Historical Telecommunications Data

The Authorised Officer must be satisfied that the disclosure of telecommunications data by the carrier or internet service provider is reasonably necessary for the enforcement of the criminal law (s. 178) or for the enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue (s. 179). This is the same as the test previously applied under s. 282 of the *Telecommunications Act 1997*.

s37(2)(b)

Access to Prospective Data

The briefing paper must address in terms of the rational for disclosure of the telecommunications data, the test established by s. 180 of the *Telecommunications (Interception & Access) Act 1979* (TIA Act). s37(2)(b)

s37(2)(b)

s37(2)(b)

Applications for Revocations

Revocations are only relevant to the access to prospective data.

Section 183 of the *Telecommunications (Interception & Access) Act 1979* (TIA Act) provides that a revocation and notification of a revocation by the Australian Security Intelligence Organisation or a criminal law-enforcement agency must comply with any requirements determined by the Communications Access Coordinator (CAC) and be in either written or electronic form.

s37(2)(b)

s37(2)(b)

s37(2)(b)

s37(2)(b)

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

Financial approval is subject to the *Financial Management and Accountability Act 1997*, FMA Regulations and FMA Orders s47E(d)

s47E(d)

s47E(d)

Authorisation Forms

Section 183 of the *Telecommunications (Interception & Access) Act 1979* (TIA Act) provides that all authorisations, notifications and revocations for access to telecommunications data must comply with such requirements as determined by the Coordinator Access Control (CAC).

s37(2)(b)

s47E(d)

Reporting

The AFP is required to report annually (no later than within 3 months of the end of the financial year) to the Attorney-General regarding its access to telecommunications data.

The AFP's report must include statistics on the number of authorisations made during the previous financial year for:

- The disclosure under s. 178 of existing telecommunications data for the enforcement of the criminal law
- The disclosure under s. 179 of existing telecommunications data for the purpose of enforcing a law imposing a pecuniary penalty or the protection of the public revenue
- The disclosure under s. 180 of prospective telecommunications data for the enforcement of the criminal law
- Any other matter requested by the Minister in relation to those authorisations.

The Attorney-General will then compile the reports of all enforcement agencies into annual report for Parliament.

s47E(d)

s47E(d)

s47E(d)

Section 185 of the *Telecommunications (Interception & Access) Act 1979* (TIA Act) stipulates that all Authorisations are to be retained by the Requesting Agency for a period of no less than 3 years.

s47E(d)

s47E(d)

Further Advice

s47E(d)

On legal issues: AFP Legal.

References

- *Australian Federal Police Act 1979*
- *Financial Management and Accountability Act 1997*
- Financial Management and Accountability Regulations 1997
- *Telecommunications Act 1997*
- *Telecommunications (Interception & Access) Amendment Act 2007*
- Legislation Program Operational Summary Telecommunications (Interception and Access) Amendment Act 2007: Access to Telecommunications Data

s37(2)(b)

s37(2)(b)

s37(2)(b)

s37(2)(b)