Telecommunications Data Authorisations

Relevant Legislation and Other Links

Telecommunications (Interception and Access) Act 1979 (Cth) ("TIA Act")

Telecommunications Act 1997 (Cth) ("TA Act")

Where relevant, this Standard Operating Procedure (SOP) refers to specific provisions of the legislation. Unless otherwise indicated, such references are to sections of the TIA Act.

This Standard Operating Procedure needs to be read in conjunction with the following Standard Operating Procedures:

- Surveillance Device Warrants;
- Telecommunications Interception and Stored Communication Warrants.

Previous Versions

Nil.

Approval

This Standard Operating Procedure is approved.

Michael Griffin AM
Integrity Commissioner
28 March 2018
Templates

<table>
<thead>
<tr>
<th>No.</th>
<th>Template name</th>
<th>TRIM reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Authorisation request</td>
<td>15#8710DOC</td>
</tr>
<tr>
<td>2.</td>
<td>Notice to carrier of authorisation</td>
<td>14#2394DOC</td>
</tr>
<tr>
<td>3.</td>
<td>Revocation of prospective authorisation</td>
<td>16#1499DOC</td>
</tr>
</tbody>
</table>
CONTENTS

1.0 PURPOSE .................................................................................................................. 5

2.0 WHAT IS TELECOMMUNICATIONS DATA .................................................................. 5

3.0 GENERAL PROHIBITION ON ACCESSING DATA ................................................. 5

4.0 AUTHORISATIONS ................................................................................................... 6

  4.1 Eligibility ................................................................................................................. 6

  4.2 Existing telecommunications authorisations ......................................................... 6

  4.3 Prospective telecommunications authorisations ..................................................... 7

5.0 PRIVACY CONSIDERATIONS ................................................................................ 7

6.0 PROCESS .................................................................................................................. 8

  6.1 Authorisation ........................................................................................................... 8

  6.2 Revocation ............................................................................................................... 9

7.0 USE AND DISCLOSURE ......................................................................................... 9

  7.1 Offences – disclosure or use of information about a data authorisation ................. 9

  7.2 Offences – disclosure or use of accessed data ....................................................... 10

8.0 EVIDENTIARY CERTIFICATES ............................................................................. 10

9.0 JOURNALIST INFORMATION WARRANTS ......................................................... 11

  9.1 Background .......................................................................................................... 11

  9.2 When a journalist information warrant is necessary ............................................. 11

  9.3 Who may apply for a journalist information warrant ........................................... 12

  9.4 Public Interest Advocates ..................................................................................... 13

  9.5 Threshold for the issue of a journalist information warrant .................................... 13

  9.6 Notifying the Ombudsman .................................................................................... 13

  9.7 Entry into force and revocation ............................................................................. 14

10.0 RECORD KEEPING AND REPORTING ............................................................. 14

  10.1 Reports to the Minister ......................................................................................... 14

  10.2 Record keeping .................................................................................................... 14

11.0 INSPECTIONS BY THE OMBUDSMAN .............................................................. 15

Attachment A ................................................................................................................. 16
1.0 PURPOSE

The Parliament of Australia has provided the Integrity Commissioner and the Australian Commission for Law Enforcement Integrity (ACLEI) with sensitive, covert law enforcement powers. The use of these powers has the potential to affect privacy and other liberties of individuals.

To protect the legal rights of all parties, including ACLEI, this Standard Operating Procedure (SOP) aims to ensure that:

- accessing an individual's telecommunications data is conducted in strict accordance with the law;
- such operations are demonstrably fair; and
- appropriate records are kept to meet transparency and accountability requirements.

2.0 WHAT IS TELECOMMUNICATIONS DATA

Telecommunications data is the metadata created as a result of a communication. That is, telecommunications data is information about the communication. Data includes:

- subscriber information (such as name, address, billing or payment information);
- the source and destination of a communication;
- the date, time and duration of a communication;
- the type of communication (such as voice, SMS, email, chat, forum or social media); and
- the type of a service used (such as ADSL, Wi-Fi, VoIP, GPRS).

Importantly, telecommunications data does not include the content of a communication. For example, telecommunications data would include the information that Person A sent an email to Person B over Wi-Fi on 1 January 2016 at 10.06am. However, the text contained in that email would be outside the scope of 'data.'

3.0 GENERAL PROHIBITION ON ACCESSING DATA

The Telecommunications Act 1997 (Cth) ('TA Act') makes it an offence for a telecommunications worker to disclose communications data that the worker has accessed in the course of his or her employment (sections 276-278 TA Act). The prohibition applies to the following people (section 271 TA Act):

- a carrier;
- a carriage service provider;
• an employee of a carrier;
• an employee of a carriage service provider;
• a telecommunications contractor; and
• an employee of a telecommunications contractor.

The Telecommunications (Interception and Access) Act 1979 ('TIA Act') provides that accessing telecommunications data will not constitute an offence under the TA Act if it is done under the authority of a data authorisation (section 175).

Unless otherwise specified, references to provisions in this SOP relate to the TIA Act.

4.0 AUTHORISATIONS

4.1 Eligibility

Data authorisations may only be issued by 'authorised officers' of ACLEI. ACLEI authorised officers are:

• the Integrity Commissioner; and
• those officers authorised under section 5AB of the TIA Act (the current list can be found on the Intranet under 'ACLEI delegations and authorisations' and in TRIM folder 14/852).

ACLEI qualifies as both a 'criminal law enforcement agency' (section 110A) and as an 'enforcement agency' (section 176A) under the TIA Act for the purpose of accessing telecommunications data. This means that ACLEI authorised officers may issue both prospective and existing telecommunications authorisations.

4.2 Existing telecommunications authorisations

'Existing telecommunications data' refers to data which already exists at the point in time when an ACLEI officer notifies a telecommunications carrier of a data authorisation (section 178(2)).

An existing telecommunications authorisation may only be issued if the authorised officer is satisfied that:

(i) the disclosure of the telecommunications data is reasonably necessary for the enforcement of the criminal law (section 178(3)); and
(ii) the authorised officer is satisfied on reasonable grounds that any interference with the privacy of any person is justifiable and proportionate (see Chapter 5 below).
An authorised officer may also issue an existing data authorisation in circumstances where it is reasonably necessary for the enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue (section 179(3)).

4.3 Prospective telecommunications authorisations

'Prospective telecommunications data' refers to data that comes into existence during the period for which the authorisation is in force (section 180(2)). For example, a prospective data authorisation issued on 1 June 2018 may authorise the disclosure of any telecommunications data linked to a service which comes into existence for a future date range, for example between 4 June 2018 and 4 July 2018.

A prospective telecommunications authorisation may only be issued if the authorised officer is satisfied that:

(i) the disclosure is reasonably necessary for the investigation of:
   • a serious offence (see definition below); or
   • an offence against a law of the Commonwealth, a State or a Territory that is punishable by imprisonment for at least three years (section 180(4)); and

(ii) the authorised officer is satisfied on reasonable grounds that any interference with the privacy of any person is justifiable and proportionate (see Chapter 5 below).

A 'serious offence' is defined in section 5D of the TIA Act. It includes any offence punishable by at least 7 years imprisonment, plus an extensive list of prescribed offences. These prescribed offences include offences involving bribery or corruption of an officer of the Commonwealth, and serious fraud.

A prospective telecommunications authorisation can only authorise the disclosure of telecommunications data for a maximum of 45 days, beginning on the day the authorisation is made (section 180(6)). A journalist information warrant is an exception to this rule and may be in force for up to 90 days. Journalist information warrants are dealt with below in Chapter 9.

Since the threshold for issuing a prospective data authorisation is higher than the threshold for issuing an existing data authorisation, an authorisation for prospective data may also authorise the disclosure of existing data (section 180(3)).

5.0 PRIVACY CONSIDERATIONS

Before an authorised officer issues a data authorisation, he or she must be satisfied on reasonable grounds that any interference with the privacy of any person(s) is
justifiable and proportionate, having regard to certain matters including (section 180F):

- the gravity of any conduct in relation to which the authorisation is sought, including the seriousness of the relevant offence;
- the likely relevance and usefulness of the information or documents; and
- the reason why the disclosure is proposed to be authorised.

These considerations must be explicitly dealt with in the data authorisation. ACLEI's template for data authorisations contains a free text area for privacy considerations. This should be completed by the case officer for consideration by the authorising officer. The amount of detail required will depend on the extent to which an individual's privacy is being infringed and the seriousness of the offence being investigated.

6.0 PROCESS

6.1 Authorisation

The case officer must complete an internal Telecommunications Request – Authorisation Record using ACLEI's template. It is ACLEI practice that a single authorisation may cover data in relation to more than one telecommunications service, so long as the data is being sought for the same reason and the same privacy considerations apply.

The authorisation record is then submitted to an authorised officer for approval.

Details are to be entered into the Data Retention Register located in TRIM (refer document 15#8621DOC) and each record is to be given a unique ACLEI identification number, which is to be recorded on any documentation associated with that request. This practice will assist with tracking any requests, as well as for billing purposes.

Except when an IPND check is requested, the requesting officer will prepare an authorisation advice to send to the relevant telecommunications carrier. This is to notify the carrier that access to the telecommunications data has been authorised (section 184(3),(4)).

For existing data authorisations, the case officer will be responsible for sending the external authorisation advice to the carriage service provider. The carriage service provider will then send the relevant data to ACLEI.

For prospective data authorisations, the Assistant Director Operational Support will prepare the external minute and provide it to the assisting agency. The assisting agency will liaise with the carrier and make the data available to ACLEI via the respective application to which approved ACLEI officers have access (in the case of
the AFP, this would be the AFP ETS system, to which the AFP has approved access for certain ACLEI officers).

For IPND checks, an external notice to the carrier service provider does not need to be prepared. After a request is approved by the authorised officer or an officer with user access, the authorising officer or an officer with user access will access the IPND information from a computer terminal within ACLEI and provide the data to the case officer.

This process is set out in a diagram at Attachment A.

6.2 Revocation

A prospective authorisation must be revoked if the authorised officer is satisfied that the grounds for originally issuing the data authorisation cease to exist (section 180(7)).

In the case of a revocation, a relevant staff member of ACLEI must notify the person who was originally notified of the authorisation. This will usually be either the carrier or the assisting agency (section 184(4)).

7.0 USE AND DISCLOSURE

7.1 Offences – disclosure or use of information about a data authorisation

Generally, it is an offence to use or disclose any information which would reveal the existence of a telecommunications data authorisation.

Specifically, it is an offence to disclose or use information about (section 181B(1),(4)):

- whether a telecommunications data authorisation has been, or is being sought;
- the making of such an authorisation;
- the existence or non-existence of such an authorisation;
- the revocation of such an authorisation; and
- the notification of such a revocation.

It is also an offence for a person to disclose or use a document if that document is an authorisation, a revocation of an authorisation or a notification of a revocation (section 181B(2),(5)).

These offences each carry a penalty of 2 years imprisonment.

However, the use or disclosure of such information or documents will not be an offence if (section 181B(3),(6)).
• the disclosure or use is for the purposes of the authorisation, revocation or notification concerned; or
• the disclosure or use is reasonably necessary for the enforcement of the criminal law (amongst other things).

The legislation does not limit the class of persons who may receive information or documents which are lawfully disclosed.

7.2 Offences – disclosure or use of accessed data

It is an offence to use or disclose a document or information which has been disclosed to a person under a data authorisation (section 182(1)). The penalty is 2 years imprisonment.

However, the use or disclosure of such information or documents will not be an offence if (s182(2),(3)):

• if it is reasonably necessary for the enforcement of the criminal law; or
• it is reasonably necessary to comply with relevant reporting obligations under the TIA Act.

The legislation does not limit the class of persons who may receive information or documents which are lawfully disclosed.

8.0 EVIDENTIARY CERTIFICATES

An evidentiary certificate may be admitted in evidence in exempt proceedings as proof of its contents.

'Exempt proceedings' are defined to include police disciplinary proceedings, a proceeding to terminate the employment of a police officer or police employee and other proceedings (excluding prosecution) relating to alleged misbehaviour, or alleged improper conduct, of an officer of the Commonwealth or of a State (s 5B).

Certain individuals who work for a carrier may issue an evidentiary certificate. A carrier's evidentiary certificate may set out the facts concerning the acts or things done in giving effect to a data authorisation (s 185A(1)).

An ACLEI certifying officer may also issue an evidentiary certificate. An ACLEI evidentiary certificate may set out facts with respect to (s 185C(1)):

• the things done in giving effect to a data authorisation;
• the communication by that person of information which is covered by a data authorisation;
• the use of information covered by a data authorisation;
• the recording of information covered by a data authorisation;
An ACLEI 'certifying officer' is the Integrity Commissioner or an SES employee with an authorisation under section 5AC(2) of the TIA Act. A current list of authorised employees is available on the Intranet. The Assistant Director Operational Support will assist in facilitating requests for evidentiary certificates.

9.0 JOURNALIST INFORMATION WARRANTS

9.1 Background

It is essential that all ACLEI staff members who have the authority to apply for a Journalist Information Warrant read and understand section 180H of the TIA Act. If uncertain of any aspect of the regime advice must be sought from the Legal Section.

On 13 October 2015, a higher threshold was introduced for instances where metadata was being sought in relation to a journalist for the purpose of identifying that journalist's source. The Journalist Information Warrant provisions were introduced into the TIA Act in recognition of the public interest in protecting journalists’ sources while ensuring agencies have the investigative tools necessary to protect the community. These provisions require an application to be made to an issuing authority such as an eligible Judge or Administrative Appeals Tribunal Member. Applications for a warrant are also subject to scrutiny by a Public Interest Advocate, who is appointed by the Prime Minister under the TIA Act. These oversight mechanisms aim to ensure that access to such data is only permitted in circumstances where the public interest in the issuing of the warrant outweighs the public interest in maintaining the confidentiality of the source.1

9.2 When a journalist information warrant is necessary

The authorisation system described so far in this SOP changes in particular circumstances involving a journalist. If an authorised officer knows, or reasonably believes, that the subject of the data authorisation would be:

- a person who is working in a professional capacity as a journalist, or an employer of such a person; and
- the purpose of making the authorisation would be to identify the journalist's source

---

1 A report on the Commonwealth Ombudsman's inspection of the Australian Federal Police under the Telecommunications (Interception and Access) Act 1979, October 2017
then the authorised officer must not issue a data authorisation unless a journalist information warrant is in force (section 180H).

In respect to when a Journalist Information Warrant is needed on 26 April 2017, the AFP advised the Commonwealth Ombudsman's office that it had breached the TIA Act, as it had accessed metadata pertaining to a journalist without obtaining a Journalist Information Warrant.

There were four authorisations associated with the breach:

- one authorisation that was in clear breach of s 180H of the TIA Act, in that it was in relation to the journalist for the purpose of identifying that journalist's source
- one authorisation that preceded the above authorisation and was in relation to the journalist, but did not directly identify that journalist's source
- two authorisations that were issued subsequent to the authorisation in breach that were not directly made in relation to the journalist (or their employer) but were for the purpose of identifying that journalist's source.

The Ombudsman thought it was arguable whether three of the above four authorisations (the one preceding and the two subsequent) breached the relevant provisions of the TIA Act. However, by the time of their inspection, the AFP had taken remedial action in relation to all four authorisations to limit any direct or indirect use of the obtained metadata. The breach/breaches were scrutinised by the Ombudsman who drafted a public report with a number of recommendations for how the AFP could improve its practice and procedure.

As such, it is important that the requirements for a Journalist Information Warrant are carefully considered wherever a warrant is sought in relation to a journalist, and the Legal Section is consulted.

9.3 Who may apply for a journalist information warrant

An ACLEI officer who is authorised under section 39(2)(aa)(iii) of the TIA Act may apply to an issuing authority for a journalist information warrant (section 180Q). Those ACLEI officers with current section 39(2)(aa)(iii) authorisations are listed on the intranet. An 'issuing authority' is defined in section 6DB to include judges and nominated members of the Administrative Appeals tribunal.
9.4 Public Interest Advocates

Public Interest Advocates are appointed by the Prime Minister.

A Public Interest Advocate may make submissions to an issuing authority about matters relevant to a decision to issue or refuse a journalist information warrant, or possible conditions or restrictions to be placed on the warrant (section 180X).

9.5 Threshold for the issue of a journalist information warrant

Journalist information warrants are issued under section 180T of the TIA Act. An issuing authority may only issue a journalist information warrant if satisfied that the warrant is reasonably necessary for the enforcement of the criminal law, and the public interest in issuing the warrant outweighs the public interest in protecting the confidentiality of the identity of the relevant journalist source, having regard to:

- privacy implications;
- the gravity of the matter;
- the extent to which the data would be likely to assist in the matter;
- whether reasonable attempts have been made to obtain the information by other means;
- any submissions made by a public interest advocate; and
- any other matters that the issuing authority considers relevant.

An issuing authority may require an ACLEI officer to furnish the issuing authority with particular information (section 180R) under an oath or affirmation (section 180S).

Once a journalist information warrant is issued, an authorised officer may make a data authorisation under the authority of the warrant according to normal procedures, as set out in Chapter 6 above.

9.6 Notifying the Ombudsman

If a journalist information warrant is issued, the Integrity Commissioner must give a copy of the warrant to the Commonwealth Ombudsman as soon as practicable (section 185D(5)(b)).

If a data authorisation is made under the authority of a journalist information warrant, the Integrity Commissioner must give a copy of the authorisation to the Commonwealth Ombudsman as soon as practicable after the warrant has expired.
9.7 **Entry into force and revocation**

A journalist information warrant enters into force when it is issued (section 180V). It will remain in force for the period specified in the warrant, up to a maximum period of 90 days (section 180U).

The Integrity Commissioner may revoke a journalist information warrant at any time by means of a signed revocation instrument (section 180W(1)(a)). The Integrity Commissioner must revoke a journalist information warrant if he or she is satisfied that the grounds on which the warrant was issued have ceased to exist (section 180W(1)(b)).

10.0 RECORD KEEPING AND REPORTING

10.1 **Reports to the Minister**

The Integrity Commissioner must report annually to the Minister for Justice on a number of matters associated with data authorisations (section 186). This report must be made as soon as practicable after 30 June each year, and within 3 months of 30 June at the latest. In particular, the Integrity Commissioner must report on (section 186):

- the number of authorisations made;
- the offences in respect of which authorisations were made;
- the age of the data sought under an authorisation;
- the number of authorisations for subscriber information;
- the number of authorisations for traffic data; and
- the number of authorisations that were made under journalist information warrants.

The Assistant Director Operational Support will prepare these reports to the Minister.

10.2 **Record keeping**

The Integrity Commissioner must keep the following records for a period of three years, or until the Ombudsman gives the Minister a report about the records, whichever is earlier (section 186A(3)):

- data authorisations;
- records which indicate whether authorisations were properly made, including in relation to the privacy requirements set out in section 180F;
- records showing that ACLEI notified the relevant carrier of an authorisation
- revocations;
- records indicating whether revocations were properly made;
- records showing that ACLEI notified the relevant carrier of a revocation;
documents or materials indicating that any use or disclosure of data
authorisation information or accessed data was lawful;
- evidentiary certificates issued by ACLEI authorised officers; and
- reports given to the Minister under section 186.

11.0 INSPECTIONS BY THE OMBUDSMAN

The Commonwealth Ombudsman is required under Chapter 4A (sections 186B-186J)
to inspect ACLEI's records to determine the extent of compliance with the data
provisions of the TIA Act. The Ombudsman has extensive powers to enter premises
and examine records and reports to the Minister about his or her inspections.

Consequently personnel from the Commonwealth Ombudsman office will attend
ACLEI periodically to inspect the records. The Ombudsman's staff should have
unrestricted access to ACLEI's records related to TI. ACLEI staff must provide the
Ombudsman's inspectors with all necessary assistance to enable them to perform
their duties.

The Assistant Director Operational Support will facilitate any visit by the
Commonwealth Ombudsman for the purpose of record inspection.

The Commonwealth Ombudsman will report to the Minister about the results of its
inspections.
**AUTHORISATION REQUEST PROCESS**

- Authorisation record is completed by case officer.
- Authorisation record is approved by the authorised officer.
- Authorisation record is not approved by the authorised officer.

**IPND Checks**
- Authorised Officer or officer with user account access accesses the IPND information and provides it to the case officer.

**Existing data**
- Authorised officer approves a 'authorisation advice' to the carrier.
- Operations Support Officer provides the 'authorisation advice' to the carrier.
- Carrier provides data to ACLEI.

**Prospective data**
- Authorised officer signs off an external minute to the CSP.
- Assistant Director Operational Support provides the external minute to the AFP.
- AFP liaise with CSP to arrange access to data for period of the authorisation.
- AFP provides data to ACLEI via the AFP ETS application accessible to approved ACLEI officers.

**Provide documentation to the Assistant Director Operational Support.**
- No data is accessed.