Australian Government

Australian Commission for Law Enforcement Integrity

STANDARD OPERATING PROCEDURE

TELECOMMUNICATIONS DATA AUTHORISATIONS

APPROVED:
RESPONSIBILITY: OPERATIONS

Version 2

aclei.gov.au

Australian Government
Australian Commission for Law Enforcement Integrity

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

March 2018

Approval

This Standard Operating Procedure is approved.

Jaala Hinchcliffe
Integrity Commissioner

9 April 2021

Australian Government
Australian Commission for Law Enforcement Integrity

CONTENTS

1 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 DEFINITIONS

CAD	call associated data
CCR	call charge record
existing telecommunications data	data which already exists when an ACLEI officer notifies a telecommunications carrier of a data authorisation (section 178(2)).
IPND	Integrated Public Number Database which records most Australian phone numbers and owner details
Journalist Information Warrant	a warrant that must be in place before an authorisation can be made 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

LBS	Optus location based services
ping	The carrier sends an underlining management control SMS to the service which connects to the closest towers to provide longitude and latitude to create a mappable location of the service
ping frequency	the frequency in time that a ping is set
prospective telecommunications data	data that comes into existence while the authorisation is in force
SEEK	Telstra SEEK on demand locations business services
serious offence	any offence punishable by at least 7 years imprisonment, plus an extensive list of prescribed offences, including offences involving bribery or corruption of an officer of the Commonwealth, and serious fraud.
Subs check	Subscriber check
RCCR	Reverse call charge records
telecommunications data	metadata created as a result of a communication
webtrace	Reverse call charge records provided by Optus

3 TEMPLATES

The following templates to be used in relation to telecommunications data authorisations are available in **CM 20/471-1**

Template	Purpose	CM Reference
Request for existing data authorisation	This template is used to document the case officer's request to the authorised officer for an existing data authorisation. The authorised officer documents their considerations and decision on the request.	**21#9641DOC**
Request for existing data authorisation – IPND data	This template is used to document the case officer's request to the authorised officer for an existing data authorisation for IPND data. The authorised officer documents their considerations and decision on the request.	**21#9642DOC**
Request for prospective data authorisation	This template is used to document the case officer's request to the authorised officer for prospective data authorisation. The authorised officer documents their considerations and decision on the request.	**21#9643DOC**
Authorisation for access to existing information or data	This is the authorisation by the authorised officer for existing information or data.	**21#9644DOC**
Authorisation for access to existing information or data – IPND data	This is the authorisation by the authorised officer for existing IPND data.	**21#9645DOC**
Authorisation for access to prospective information or data	This is the authorisation by the authorised officer for prospective information or data	**21#9645DOC**
Notification of authorisation for existing data	This is the notification to the carrier of the authorisation. A copy of the	**21#9647DOC**

Template	Purpose	CM Reference
	authorisation is annexed to this notification	
Notification of authorisation for prospective data	This is the notification to the carrier of the authorisation. A copy of the authorisation is annexed to this notification	**21#9648DOC**
Revocation of an authorisation for access to prospective information or documents	This is the revocation by the authorised officer of a prospective information or data authorisation	**21#9649DOC**
Notification of revocation of prospective authorisation	This is the notification to the carrier of the revocation of a prospective authorisation. A copy of the revocation is annexed to this notification	**21#9650DOC**
Telecommunications data – use and disclosure log	This log is completed by the case officer each time the telecommunications data obtained under the authorisation is used or disclosed. It records the exception under the TIA Act that applies to the use or disclosure	**21#9651DOC**

4 ROLES AND RESPONSIBILITIES

Case officer	The case officer is responsible for preparing the request for authorisation and ensuring that the authorised officer has the information required in order for them to decide whether to make the authorisation. After the authorisation is made, the case officer is responsible for providing it to the Operations Support Team to process.

	The case officer is responsible for recording any use or disclosure of the material provided under an authorisation. The case officer is responsible for being available during inspections by the Ombudsman's office to discuss any authorisations requested.
Authorised officer	The authorised officer is responsible for considering requests for access to data by case officers, against the criteria set out in the TIA Act. If the authorised officer decides to grant an authorisation, the authorised officer is responsible for ensuring that the authorisation reflects the authorised officer's decision. If the authorised officer is satisfied that the grounds for a prospective data authorisation cease to exist, the authorised officer is responsible for revoking that authorisation. The authorised officer is responsible for being available during inspections by the Ombudsman's office to discuss any authorisations granted.
Operations Support team	The Operations Support team can provide assistance to the case officer in relation to requesting telecommunications data. However, it is not a requirement that the case officer must liaise with the Operations Support team prior to making a request for telecommunications data. The Operations Support team is responsible for: • Processing authorisations • Liaising with service providers • Reviewing provided data and quarantining any data which does not fall within the terms of the authorisation • Preparing reports required under the TIA Act • Liaising with the Ombudsman in relation to inspections

5 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, but does not include 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.'

If you are seeking information on the **content** of a communication, a telecommunication data authorisation is not appropriate.

Telecommunications data includes the data that is obtained from undertaking IPND checks. A telecommunications data authorisation is required before undertaking an IPND check.

Telecommunications data can provide useful information to an investigation including that contact has occurred between parties and provide details of the date, time, number called and duration. As telecommunications data includes IPND checks, it can include information on who has subscribed to a particular number.

6 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 TIA Act if it is done under the authority of a data authorisation (section 175).

Therefore, it is vital that if you want to access telecommunications data, you must comply with the provisions of the TIA Act.

7 WHO CAN AUTHORISE ACCESS TO TELECOMMUNICATIONS DATA

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

- the Integrity Commissioner; and
- those officers authorised to be "authorised officers" under section 5AB of the TIA Act (see 'ACLEI delegations and authorisations' on the intranet)

8 WHAT TYPE OF DATA CAN BE ACCESSED

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 authorisations for both existing telecommunications data and prospective telecommunications data.

9 REQUESTING ACCESS TO DATA

If a case officer wishes to access telecommunications data, they must make a request to an authorised officer. The template forms to make a request to access data are at **CM 20/471-1**. The information required to be provided by the case officer includes:

- the type of authorisation
- the type of data sought
- the services from which the data is requested
- the type of check to be undertaken (see attachment A)
- the information available to satisfy the authorised officer that the test in the TIA Act is made out including:
    - the link between the POI and the service or the link between the person to whom the service relates and the offence

- the information available to satisfy the authorised officer that the privacy considerations in the TIA Act are made out
- for existing data requests – the date range for data being sought with a justification for that date range
- for prospective data requests - the length of time that the authorisation is requested for
- an estimate of the cost of the requested data (see **CM15/554** for costs of each request)

In requesting that the authorised officer authorise access to data, the case officer must provide sufficient information in the request to enable the authorised officer to be satisfied of each of the applicable tests in the TIA Act.

If the case officer does not satisfy the authorised officer that the tests in the TIA Act have been made out, the access to the data will not be authorised.

Requests for IPND checks

It is ACLEI practice that a single authorisation for IPND checks 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. ACLEI's policy is that the limit to the number of telecommunication services that can be contained in one authorisation is 25.

If more than one telecommunication service is to be included in the one authorisation, the case officer must provide information in the request as to why the authorised officer can be satisfied of the requisite tests **for each of the services requested**. The case officer may be able to do this by providing information that indicates:

- that the services are all connected to the one person
- that the services are connected to different people but each of those people are connected to the alleged offence

If the case officer does not satisfy the authorised officer that the tests in the TIA Act have been made out in relation to a particular telecommunication service, the access to the data will not be authorised.

Requests for IPND checks must also include the type of check that is being requested. The five available checks are:

- Customer name to number search
- Name and address search
- Number to name search

- Number to name search with history
- Service address search

A request for an IPND check must not include a date range, as the IPND system does not provide the ability to enter a date range.

Requesting an authorisation in relation to prospective data

If the case officer is requesting an authorisation in relation to prospective data which required the assistance of an agency other than the AFP, the case officer must seek approval from the agency that they are able to provide the required assistance prior to the authorisation being signed by the authorised officer.

Requesting an authorisation in relation to a person who is working as a journalist

If the case officer is requesting an authorisation in relation to a person who is working as a journalist, consideration must be given to whether a journalist information warrant is required to be in place before an authorisation can be made. A journalist information warrant is required 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.

If the case officer considers that a journalist information warrant is likely to be required, they should immediately consult with the Legal Team. The Legal Team will work with the case officer through the steps to obtain a JIW, including seeking approval from the Integrity Commissioner prior to the warrant being sought.

10 EXISTING TELECOMMUNICATIONS DATA – AUTHORISED OFFICER CONSIDERATIONS

'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) any interference with the privacy of any person is **justifiable and proportionate**

Further information on the privacy considerations is set out 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)). The same privacy considerations apply to this authorisation.

The authorised officer records his or her decision in relation to the request for access to data in the request form. In recording their decision, the authorised officer must set out the basis on which they are satisfied of both limbs of the test.

If the authorised officer has been provided with additional information that was not included on the request form, for example through a verbal briefing by the case officer, this should be noted by the authorised officer on the request form.

If the authorised officer decides to authorise the requested access to data, the authorised officer must then complete an *Authorisation for access to existing information or data*, which is provided to the carrier as part of the notification. If the request is for an IPND check, the authorised officer completes an *Authorisation for access to existing information or data – IPND* form, which is provided to the Operations Support Team to complete the check.

If the authorised officer makes any variations or amendments by hand to the *Authorisation for access to existing information or data* form, those variations or amendments must be signed and dated.

The request form and the *Authorisation for access to existing data* can be completed electronically by the authorised officer and the authorised officer can apply their electronic signature to the forms.

Whether approved in writing or electronically, the completed forms must be saved in CM by the case officer.

11 PROSPECTIVE TELECOMMUNICATIONS DATA – AUTHORISED OFFICER CONSIDERATIONS

'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 s5D); 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.

Further information on the privacy considerations is set out below.

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 considering the request for prospective telecommunications data, the authorised officer must consider whether the length of time requested for the authorisation is appropriate.

If the authorised officer makes the authorisation, they should use a warrant date calculator to ensure that the end date for the authorisation is correctly calculated (see for example, the **AFP Warrant Date Calculator - AFP Hub > Operational info and resources > Investigators Toolkit > Special projects > Warrant date calculator**)

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)).

The authorised officer records his or her decision in relation to the request for access to data in the request form. In recording their decision, the authorised officer must set out the basis on which they are satisfied of both limbs of the test.

If the authorised officer has been provided with additional information that was not included on the request form, for example through a verbal briefing by the case officer, this should be noted by the authorised officer on the request form.

If the authorised officer decides to authorise the requested access to data, the authorised officer must then complete an *Authorisation for access to prospective information or data*, which is provided to the carrier as part of the notification.

If the authorised officer makes any variations or amendments by hand to the *Authorisation for access to prospective information or data*, those variations or amendments must be signed and dated.

The request form and the *Authorisation for access to prospective data* can be completed electronically by the authorised officer and the authorised officer can apply their electronic signature to the forms.

Whether approved in writing or electronically, the completed forms must be saved in CM by the case officer.

12 JOURNALIST INFORMATION WARRANTS

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

then the authorised officer must not issue a data authorisation unless a journalist information warrant is in force (section 180H).

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.

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 above.

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.

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)).

13 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 request by both the case officer and 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.

14 PROVIDING THE AUTHORISATION TO THE CARRIER

Once the authorisation is provided by the authorised officer, the case officer must provide a copy of the authorisation to the Operations Support Team. A member of the Operations Support team will enter the details into the Data Retention Register (**CM 15#8621**) and give each record 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.

For existing data authorisations, Operations Support will be responsible for sending the notification to the carriage service provider. The carriage service provider will then send the relevant data to ACLEI.

For existing data authorisations for IPND checks, Operations Support will be responsible for conducting the check once the authorisation is provided to them.

For prospective data authorisations, Operations Support will be responsible for sending the notification to the carriage service provider. The carriage service provider will then send the relevant data the assisting agency, who will 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).

15 PROVISION OF DATA

Data that is provided to ACLEI through an authorisation will be received by the Operations Support team. The Operations Support team will review the data received against the authorisation, to ensure that it complies with the terms of the authorisation. Any data that is provided outside of the terms of the authorisation will be quarantined by the Operations Support Team and will not be made available to the case officer.

The Operations Support team will save the material that is within the terms of the authorisation in CM and provide that data to the case officer.

16 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)).

If a case officer forms the view that the grounds for issuing the data authorisation cease to exist, they must inform the authorised officer immediately to enable the authorised officer to revoke the authorisation.

At the same time, the case officer must inform the Operations Support Team, so that the Operations Support Team can request the assisting agency of the intention to revoke,

The authorised officer should document their decision to revoke the authorisation and complete the revocation form (see **CM 21#9649DOC**).

The revocation form will be sent to the carrier and the assisting agency by the Operations Support Team (section 184(4)).

17 USE AND DISCLOSURE

It is an offence to use or disclose any information which would reveal the existence of a telecommunications data authorisation or to use or disclose a document or information which has been disclosed to a person under a data authorisation. However, there are exceptions to these offences for (amongst other things) the enforcement of criminal law. There is more information about these offences below.

In order to ensure that any use or disclosure of information is done for a proper purpose, the TIA Act requires the Integrity Commissioner to keep records of use and disclosure of information in relation to telecommunications data authorisations and telecommunications data obtained under an authorisation.

The records in relation to the disclosure of telecommunications data authorisations or telecommunications data for the purpose of the enforcement of criminal law are kept by the case officer, using the template at **CM 21#9651DOC**. The information to be recorded in the template includes:

- the disclosure or use that took place
- when the disclosure or use took place
- the CM reference to the disclosure or use
- the basis on which the disclosure or use falls within one of the exceptions

Any disclosure of the authorisation or the data, including in internal documents such as the Final Investigation Report, **must** be recorded in this template and made available for auditing purposes and inspections by the Ombudsman.

A link to the saved disclosure log in CM should be sent to the Operations Support Team.

Offences – disclosure or use of information about a data authorisation

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.

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.

18 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)).

If the case officer requires an evidentiary certificate, the case officer will email Operations Support Team with a request including the following information:

- Carriage Service Provider
- Date certificate required by
- Original Law Enforcement Agency request reference
- Original Carriage Service Provider reference
- Original Request Type e.g CCR, subscriber check
- Service identifier (number)
- State jurat required to be used in the certificate

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;
- the custody of a recording of information covered by a data authorisation; and
- the giving in evidence 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.

19 RECORD KEEPING AND REPORTING

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, for approval by the Integrity Commissioner.

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.

20 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, including providing access to Ombudsman inspection staff to ACLEI ICT systems to enable the inspection to be conducted.

Case officers who have requested access to data and authorised officers will make themselves available to inspectors at any time during an inspection.

The Commonwealth Ombudsman will report to the Minister about the results of its inspections.

Australian Government
Australian Commission for Law Enforcement Integrity

Attachment A – Types of data

The Operations Support team can provide information on the different types of data that can be obtained through a data authorisation. Some examples include:

Basic subscriber – customer name, date of birth, billing address, date of connection/disconnection

Call records – calling party (A), called party (B), time, date, duration and type of call

Other call record types include:

- Cell ID location (identify base station details using a cell ID as the search criteria)
- Cell dump (identify all calls made through a cell tower. A quote must be obtained before an authorisation is made)
- VLR/GPS (near real time location of mobile if switched on and roaming)

Complex subscriber – All the information contained in a basic subscriber but the requesting officer must include details of the additional information being sought e.g copy of contract

Internet requests – these types of request require the username which is then used to request data usage/additional account details.