Accessing stored communications from a Telecommunications Carrier: Guidance

Overview

Enforcement agencies such as the ACCC must obtain a stored communications warrant to access voicemail, SMS, MMS and email communications from a telecommunications carrier without the knowledge of the sender or intended recipient.
This regime for accessing stored communications came into effect on 13 June 2006 and is regulated by Chapter 3 of the *Telecommunications (Interception and Access) Act 1979* (TIA Act).
The ACCC can only apply for a stored communications warrant in relation to:

serious contraventions, set out in section 5E of the TIA Act, rendering a person subject to a criminal fine or pecuniary penalty equivalent to at least $19,800 (individuals) or $99,000 (businesses). The following provisions meet these thresholds:

- the civil penalty provisions in Part IV of the *Competition and Consumer Act 2010* (formerly the *Trade Practices Act 1974*) and the Competition Codes
- certain civil penalty provisions and criminal offences in the Australian Consumer Law
    - consumer and business unconscionable conduct provisions
    - false or misleading representations, bait advertising, full cash pricing, pyramid selling, referral selling, harassment and coercion
    - supply or export of goods which do not comply with a product safety standard, have been declared unsafe, have been banned or don't meet the mandatory standards

serious offences, set out in section 5D of the TIA Act, and includes the criminal offences in Division 1 of Part IV of the CCA and the Competition Codes, and section 79 of the CCA relating to the making of and giving effect to a cartel provision.

Where the ACCC accesses stored communications via a stored communications warrant, it must comply with record-keeping, destruction and reporting obligations. ACCC records may be periodically inspected by the Commonwealth Ombudsman.

In what circumstance does the regime apply?

Where the ACCC wishes to access a stored communication from a carrier in a covert manner, it must apply to an issuing authority for a stored communications warrant.

What is a stored communication?

A communication is defined broadly to mean a conversation or message, a part of a conversation or message, in any form or any combination of forms.
A stored communication is a communication which has the following three

elements:

Is not passing over a telecommunications system:

- Communications that are passing over a telecommunications system must be 'intercepted' via a telecommunications interception warrant (which is not available to the ACCC).
- Communications that have never passed over a telecommunications system (for example draft emails never sent) are not subject to the new regime.
- A communication starts 'passing over' a telecommunications system when it is sent and continues until it becomes accessible to the intended recipient. There is no requirement that the intended recipient has actually accessed the communication or is even aware of the existence of the communication – it is deemed to be accessible when it has been received or delivered to the telecommunications service of the intended recipient or is under the control of the intended recipient.

Is held on equipment that is operated by and in the possession of a carrier: To be held by a carrier, the communication must have passed over a telecommunications system at some point. The stored communications regime only applies where agencies obtain access to such communications via a carrier. Communications not held by a carrier (for example those stored on a non-carrier corporate IT system, a personal hard drive or printed versions on file), are not regulated by this regime.

Cannot be accessed on that equipment by a person who is not a party to the communication without the assistance of an employee of the carrier: This further reinforces that the regime only applies where agencies obtain access to such communications via a carrier.

This definition was deliberately drafted to be technologically neutral, so any form of communication with the above three elements is included. It is therefore impossible to exhaustively list the types of stored communications.

- Clear examples of stored communications include
  - emails,
  - voicemail,
  - SMS and MMS, and
  - voice over internet protocol (VoIP) messages held by a carrier.

Under sections 110 and 116 of the TIA Act, a warrant can only be applied for and issued 'in respect of a person'. Interpretation by the Commonwealth Ombudsman and Attorney-General's Department is that TIA Act warrants may only be sought in relation to individual human beings.

How can stored communications be accessed?

Accessing a stored communication consists of listening to, reading or recording a communication.
Broadly, there are two ways that stored communications can be accessed – covertly and overtly.

Covert access occurs through a telecommunications carrier without the knowledge of the sender or the intended recipient. This form of access can only be achieved via a stored communications warrant and is most likely to be used where the ACCC has concerns that the stored communication will be deleted if the intended recipient and/or sender were made aware of our interest.

Overt access occurs via other lawful means with the **knowledge of the sender or intended recipient**. In most cases, this would involve obtaining the communication directly from the sender or intended recipient (via a statutory notice under s.155 of the CCA). However, the TIA Act also allows communications to be accessed from a carrier with the knowledge of the intended recipient.

This guidance only relates to covert access using a stored communications warrant. Questions relating to overt access should be directed in the first instance to TPLU.

What factors are relevant to the issuing authority's consideration?

The TIA Act sets out a number of factors the issuing authority must have regard to, and in summary include:

- the privacy considerations arising from the use of stored communications warrant to access a person's stored communications
- the gravity of the conduct constituting the serious offence
- how much the information sought is likely to assist the investigation
- the extent that other methods are available or have been used by the agency to gather the information
- how much these other methods are likely to impact on the investigation.

What are the internal processes to seek approval to access a stored communications warrant?

In the normal course, staff should seek approval from the Enforcement Committee to seek a stored communications warrant.

Given the transitory nature of stored communications there may be circumstances where an urgent application for a stored communications warrant may be required. In these circumstances, please contact the Group General Manager - Enforcement Operations.

We ask that staff consult the Stored Communications Warrant Checklist. The checklist is broken down in phases, with the expectation that you will complete each section at the relevant time.

How do I covertly access stored communications?

Overview

A broad overview of the steps that must be followed in order to covertly access stored communications follows. If you are considering applying for a stored communications warrant, you **must** complete the Stored

Communications Warrant Checklist.

Obtain the warrant: a written application and affidavit must be made to the issuing authority unless the matter is urgent, in which case the application may be made by phone but the affidavit must nevertheless be supplied within one day of issuing the warrant.

Notify the carrier(s) (who will execute the warrant): carrier must be notified forthwith of the issue of the warrant and be given a certified copy as soon as practicable.

Internal monitoring: internal practices and procedures must ensure that: the authority of the warrant is not exceeded; the warrant is revoked if the grounds for issuing it cease before expiry; and that the information accessed is only dealt with as allowed under the TIA Act.

Maintenance of records: documents connected with the issue of warrants must be retained for inspection by the Commonwealth Ombudsman.

Destruction of records: information or records of stored communications must be destroyed where no longer required.

Periodic reports: annual reports to the Attorney-General are required in relation to the destruction of records, certain statistics and information about the effectiveness of warrants.

Obtaining the warrant

To issue a warrant, the issuing authority (D11/2294770) will need to be satisfied that the information likely to be obtained by accessing stored communications is likely to assist the investigation of a serious contravention such as a contravention or serious offence - see details outlined above.

- For **ordinary matters**, you will need to prepare an application, affidavit and warrant for the consideration of the issuing authority.
- For **urgent matters**, an application may be made by telephone, but the written documentation will need to be lodged within one day of the issue of the warrant otherwise the issuing authority can revoke the warrant.

Where a warrant is sought in relation to a criminal investigation or an investigation where a criminal prosecution may result, the Commonwealth Director of Public Prosecutions (CDPP) should normally be contacted beforehand if the ACCC wishes to request that the CDPP settle the documentation and appear with the applicant before the issuing officer. Liaise with the Group General Manager - Enforcement Operations who will assist in processing an application for a stored communications warrant for submission to the issuing officer.
Key points:

- Applications may be made by the Chairman or a person nominated by the Chairman.
- The applicant must be present when the issuing officer considers the written application or make the telephone call for urgent applications.
- There is no prescribed form for the application although the TIA Act

requires that it set out certain information.

- The application must be accompanied by an affidavit setting out the facts and other grounds on which the application is based. There may be more than one affidavit provided and the issuing authority may require the provision of further information.
- The form of the warrant is prescribed in the Regulations and must be used. As some fields can be omitted/revised where appropriate it is important that it be reviewed before submitting to the issuing officer.

Executing the warrant

A stored communications warrant is executed by the carrier accessing the stored communications pursuant to the warrant. The carrier is required to access stored communications within the five day period the warrant is in force.
Once the warrant has been issued, you must:

- Notify the carrier(s) immediately and without delay of the issue of the warrant (usually this would be within 48 hours of the issue of the warrant).
- Give the carrier a certified copy of the warrant as soon as practicable (note: a certifying officer must certify the copy).

Internal monitoring

Once a warrant has been executed, the applicant and his or her respective branch are responsible for ensuring the following.

- The authority of the warrant is not exceeded: if the warrant is issued subject to certain conditions or restrictions, you must ensure they are adhered to.
- The warrant is revoked if the grounds for issuing it cease before expiry: the grounds for issuing the warrant must be continually reviewed during the life of the warrant and where the grounds cease before it expires, the warrant must be revoked. Liaise with the Group General Manager - Enforcement Operations and TPLU if you need to revoke a warrant.
- The information accessed is only dealt with as allowed under the TIA Act: Part 3-4 of the TIA Act contains a general prohibition on 'dealing' with information obtained via the warrant unless the dealing is specifically authorised by Part 3-4. The term 'dealing' is defined broadly and includes using it within the ACCC, disclosing it outside the ACCC, making a record of the information or giving it as evidence in a proceeding. Part 3-4 contains the most complicated provisions in the TIA Act, so please read the Stored Communications Warrant Checklist and check with the Group General Manager - Enforcement Operations and TPLU before dealing with information obtained via the warrant. Part 3-4 also protects stored communications warrant information, which is defined broadly as virtually any information relating to the warrant. For example, it includes information as to the existence or non-existence of a warrant – meaning that staff must not disclose the existence or non-existence of a warrant outside the ACCC unless this form of dealing is

authorised by Part 3-4. Check with the Group General Manager - Enforcement Operations and TPLU before dealing with stored communications warrant information.

Maintenance of records

The ACCC is required to keep certain records in connection with accessing stored communications, including:

- original warrants issued to the ACCC
- instruments of revocation
- evidentiary certificates issued by certifying officers
- authorisations by the Chairman of persons allowed to receive information from a carrier obtained under a warrant and
- details of records or information destroyed in accordance with the TIA Act.

You must consult the Stored Communications Warrant Checklist and ensure all documents are stored in accordance with it and that the Stored Communications Warrant Record Log is completed. You should also keep a copy of the Stored Communications Warrant Checklist.
The Commonwealth Ombudsman may conduct periodic inspections to ensure that the ACCC is maintaining and destroying such records as required.

Storage of information and material obtained under a warrant

All information and material obtained under a stored communications warrant should be kept in the relevant ACCC office's evidence room in accordance with the ACCC's evidence handling guidelines. In addition to the maintenance of records required above, further records detailing the chain of custody of the information and material obtained under the stored communications warrant should also be kept.

Destruction of records

Consistent with the privacy objectives of the legislation, information obtained under a warrant must be destroyed where it is no longer required.
Information obtained under a warrant must be periodically reviewed by the applicant and/or his or her respective branch against the permitted purposes, and where no longer required for such a purpose, a submission made to the Chairman seeking his approval for the destruction. Once the Chairman is satisfied that it is no longer required, the material can be destroyed.
Where the Chairman is satisfied that information obtained under a warrant is no longer required for a permitted purpose (for example, certain investigations, legal proceedings or the ACCC's recordkeeping obligations) it must be destroyed forthwith in accordance with the process outlined in the Stored Communications Warrant Checklist.
You must liaise with the Group General Manager - Enforcement Operations prior to destroying any such material.

Periodic reports

The Chairman is required to provide periodic reports to the Attorney-General in relation to the destruction of records, certain statistics and the effectiveness of warrants. The specific requirements are summarised below.

By 30 September each year, the Chairman is required to report the following to the Attorney in relation to the previous financial year:

the extent to which information was destroyed under s.150 of the TIA Act
statistics about the number of applications made and warrants issued (including telephone and renewal applications) and the number of warrants issued subject to conditions or restrictions
the number of arrests made on the basis of information accessed via a warrant and
the number of concluded legal proceedings in which information accessed via a warrant was given in evidence.

The information referred to in 2-4 above forms part of the annual report prepared by the Attorney in respect of interceptions and accessing stored communications under the TIA Act. The ACCC must provide a 'nil' report in the event that it has not made any applications, obtained warrants or destroyed material.
To ensure the accuracy of this report, you must complete the Stored Communications Warrant Checklist for each stored communications warrant that is applied for. This includes completing the Stored Communications Warrant Record Log, and notifying the Executive Office, Enforcement and Compliance Division of possible applications for stored communications warrants.

Other information

What does the warrant authorise?

A stored communications warrant authorises the ACCC to access stored communications in respect of a person (individual or company).
This means that a single warrant may be used to access stored communications held by multiple carriers and/or in relation to multiple accounts or services operated by one carrier.
Where the identity of the person is not known, the stored communications warrant must contain sufficient information to enable the telecommunications service to be identified (for example "an unknown person in respect of email address jane.doe@doe.com.au").

Duration of warrant & obtaining further warrants

A stored communications warrant is in force until it is first executed (in the case of multiple carriers until executed on the last carrier) or five days after the day on which it was issued, whichever occurs first.
This means that a carrier is only able to give access to stored communications in existence at the time the carrier was first notified of the warrant. Keep in mind that most carriers only hold stored communications for a short period before they are permanently destroyed.
Where you seek a further warrant relating to the same telecommunications service as in a previous warrant, the TIA Act precludes the issue of such a warrant until the expiration of 3 days after the day on which the previous warrant was last executed. This is to stop enforcement agencies from being

able to access stored communication in real time (that is, intercepting via the stored communications regime).

Example
On 1 August the ACCC obtains a warrant in respect of John Citizen born 22 April 1965.
The warrant authorises access of stored communications held by multiple carriers as the ACCC's investigation reveals that Mr Citizen has the following telecommunication services:
1. A home telephone with Telstra which has a voicemail facility,
2. A mobile telephone with Optus which is likely to have SMS messages, and
3. An internet account with Bigpond.
On 2 August at 9.30am the warrant is executed by notifying the Managing Directors of Telstra and Optus of the issue of the warrant. Telstra and Optus are only allowed to give the ACCC stored communications in connection with Mr Citizen that exist at the time of execution.
If on 3 August you become aware that Mr Citizen also has an additional mobile telephone with Vodafone, you can lawfully seek access to any stored communication in connection with the service by notifying the Managing Director of Vodafone of the issue of the warrant. As above, Vodafone is allowed to give the ACCC stored communications in connection with the service that exist at the time the warrant is executed.
To access further stored communications relating to Mr Citizen in relation to the same telecommunications services, a further warrant cannot be issued until 7 August (that is, three days after the warrant was last executed on 3 August).
Top

Where do I go for more information or if I need help?

In the first instance, contact the Group General Manager - Enforcement Operations who will then facilitate discussions with TPLU as required.

Critical Documents

Stored Communications Warrant Checklist
Stored Communications Warrant Record Log

Australian Competition & Consumer Commission

Stored communications warrant: checklist

Prior to obtaining the warrant:

- ☐ Read *Accessing stored communications from a telecommunications carrier* (the guidance).
- ☐ Consider whether your matter meets the requirements for a stored communications warrant under Part 3-3 the TIA Act. Specifically, you **must** read:
    - section 116
    - section 5E – serious contraventions, and
    - section 5D – serious offences.
- ☐ Under sections 110 and 116 of the TIA Act, a warrant can only be applied for and issued 'in respect of a person'. Interpretation by the Commonwealth Ombudsman and Attorney-General's Department is that TIA Act warrants may only be sought in relation to individual human beings.
- ☐ Ordinarily you should bring the matter before the Enforcement Committee, by way of a short paper if it is not otherwise being brought before the Committee, for endorsement of the proposal to seek a stored communications warrant. However, this may not be appropriate in all circumstances and you should liaise with the Group General Manager – Enforcement Operations Group about whether other options such as an oral update or out-of-session consideration are warranted.
- ☐ You **must** advise a member of the Executive Office, Enforcement and Compliance Division of your intention to seek a stored communications warrant as soon as practicable.
- ☐ You will require an application, affidavit and warrant (using available templates), which must be prepared in accordance with the TIA Act and the guidance material.
- ☐ You **must** involve CCLU with drafting this documentation. CCLU should be involved as early as possible and provided with a brief background to your matter (usually by phone or in a face to face meeting).
- ☐ The affidavit should address the issues outlined in section 116 of the TIA Act.
- ☐ The project team must ensure all relevant authorisations/appointments from the Chairman are in place by checking the delegations, instruments and authorities register. This includes:
    - that the application is made by a person a nominated to do so (s110)
    - if the application is made by telephone, the applicant is authorised to do so (s111)

- the person nominated to receive the information from the carrier is authorised to do so (s135)
- the person certifying the warrant is nominated to do so (s5)
- the person/s listening to, reading or recording a stored communication (sometimes referred to as exercising the authority of the warrant) are authorised to do so (s127)
- the person revoking a stored communications warrant is delegated to do so (s122).

You can check each of these at the Delegation, Authorisation and Appointment Register. If you require a new authorisation/appointment, templates are available. These must be settled by CCLU.

☐ The warrant must also be reviewed by your branch General Manager or Regional Director prior to its submission to the issuing officer. A copy of this checklist must be provided along with your draft documentation to your General Manager or Regional Director.

Obtaining the warrant

☐ A stored communications warrant is issued by an issuing authority. To have it issued, you must telephone the issuing authority and make an appointment with them.

☐ The person applying for the warrant (the deponent of the affidavit), the director and a CCLU lawyer would ordinarily attend the meeting with the issuing authority.

Immediately after obtaining the warrant

☐ Under a stored communications warrant, the carrier is required to access stored communications within the five day period the warrant is in force. A warrant is in force from the time it is issued to the ACCC until either it is executed by the carrier (that is, the stored communications are accessed) or the end of five days, whichever occurs earlier.

☐ An authorised representative of the carrier must be informed immediately and without delay (usually within 48 hours) of the issue of the warrant. You should contact the carrier prior to providing them with the warrant to obtain the details of their representative who is authorised to receive the warrant. Contact details:

- Telstra Law Enforcement Liaison: 03 9632 8565
- Optus Law Enforcement Unit: 02 8082 0087
- TPG Internet Law Enforcement Liaison: 02 9878 3877
- Vodafone Hutchison Law Enforcement Liaison Unit: 02 9412 8835
- Other – please contact Richard Fleming ext 1278.

☐ The following must be provided to a carrier as soon as practicable (usually within 48 hours):

- a copy of the warrant, certified in writing by a certifying officer
- a *Response to a stored communications warrant issued under the TIA Act* coversheet

- a template letter requesting that the carrier:

  - provide any documents they produce in response to the warrant on one or more compact discs or DVDs

  - deliver the disc/s to the evidence officer in the relevant ACCC office

  - certify that the documents provided in response to the warrant fall within the scope of the warrant

  - complete the *Response to a stored communications warrant* coversheet.

☐ Complete the Stored Communications Warrant Log and send to the Deputy General Manager, Executive Office, Enforcement & Compliance Division. Please include in your covering e-mail confirmation that you have completed this checklist.

☐ Store together in your office's evidence room in accordance with the Evidence Handling Guidelines the original warrant, application and affidavit and all materials obtained under the warrant. These materials must not be entered into DORIS, TRIM or Ringtail without prior discussion with the Deputy General Manager, Executive Office, Enforcement & Compliance Division.

☐ Ensure the authority of the warrant is not exceeded through the carrier producing material falling outside the scope of the warrant. If such material is produced you should notify the Group General Manager – Enforcement Operations Group.

☐ If there is material which falls outside the scope of the warrant, it will ordinarily require immediate quarantining by copying material falling within the warrant onto a separate disc(s) and following the destruction process below to destroy the original disc obtained from the carrier.

☐ During the life of the warrant, continually review grounds for issuing. If the grounds cease before it expires, the warrant must be revoked.

Dealing with information obtained under the warrant

☐ Ensure that information accessed is only dealt with as permitted under the TIA Act, which includes being for:

1) purposes connected with:

   (a) an investigation by the ACCC or another enforcement agency of a contravention which is a serious offence **or** an offence punishable by:

- imprisonment for a period, or a maximum period, of at least 12 months
- a fine of at least $6 600 for an individual
- a fine of at least $33 000 if the offence cannot be committed by an individual

(b) an investigation by the ACCC or another enforcement agency of a contravention which could, if established, render the person liable for a pecuniary penalty of at least $6 600 for an individual or $33000 if the contravention cannot be committed by an individual

(c) the making by an authority, body or person of a decision whether or not to begin a proceeding for:
- prosecution for an offence of a kind referred to in (a) above
- the confiscation of property or for the imposition of a pecuniary penalty
- recovery of a pecuniary penalty for a contravention referred to in (b) above

(d) a proceeding as outlined in (c) above.

2) giving evidence in an exempt proceeding, which includes:

- a proceeding by way of a prosecution for an offence punishable:
  - by imprisonment for a period, or a maximum period, of at least 12 months; or
  - by a fine, or a maximum fine, of at least $6 600 for an individual; or
  - if the offence cannot be committed by an individual—by a fine, or a maximum fine, of at least $33 000; or
- a proceeding for the confiscation or forfeiture of property, or for the imposition of a pecuniary penalty, in connection with the commission of such an offence; or
- a proceeding for recovery of a pecuniary penalty for a contravention that would, if proved, render the liable to:
  - a pecuniary penalty, or a maximum pecuniary penalty, of at least $6 600 for an individual; or
  - if the contravention cannot be committed by an individual—a pecuniary penalty, or a maximum pecuniary penalty, of at least $33 000.

3) record keeping (see 'Maintenance of Records' below)

4) inspection by the Ombudsman (see 'Maintenance of Records' below).

Storage

- ☐ Information or records obtained by accessing a stored communication must be stored in the relevant ACCC office's Evidence Room.
- ☐ The fact of a stored communications warrant, and any information received by accessing a stored communication must not be disclosed to anyone outside the ACCC and should only be communicated internally on a need-to-know basis.
- ☐ Material derived under the warrant is to be shaded when referred to in any staff papers.
- ☐ You should avoid making copies of information or records as far as possible. Where a working copy must be made, it is to be stored in your office's Evidence Room overnight and a record kept of its whereabouts at all times.
- ☐ Information obtained under a stored communications warrant should only be included in Enforcement Committee papers or Reason to Believe minutes where it is materially relevant to an issue and it is not possible/appropriate to exclude. Please remember that you will need to follow the destruction process outlined below should the information no longer be required in the future. To assist with the destruction process, you should update the stored communications warrant record log to list the locations of any such secondary material. Consider use of schedules or oral references to assist in identification and later destruction or to avoid unnecessary replication.
- ☐ If you are considering providing information or records to external lawyers, you **must** read section 139(2) of the TIA Act and determine, with your director, whether such communication is permitted. The following paragraphs are to be included in your covering letter to legal counsel:

  The material provided at [Attachment A / Annexure A / on disc A] is information obtained by the ACCC accessing a stored communication using a stored communications warrant pursuant to Chapter 3 of the Telecommunications (Interception and Access) Act 1979 (the TIA Act) . This information is provided to you under section 139(2) of the TIA Act to enable your office and counsel to provide legal advice to the ACCC. This information is provided on the understanding that your office and counsel will deal with it strictly in accordance with the TIA Act.

  In this regard, I request that you avoid making copies of the material. In circumstances where you consider that copies must be made, please contact [name of staff member]. Where copies are made, I request that you keep a record and that, at the finalisation of this matter, all copies of this material are provided to the ACCC.

- ☐ If you have any questions about dealing with information obtained by accessing a stored communication, you should consult with either the Group General Manager – Enforcement Operations Group or CCLU.

Maintenance and retention of records

- ☐ The following documents are to be <u>retained</u> for inspection by the Commonwealth Ombudsman and stored in your office's Evidence Room in accordance with Evidence Handling Guidelines:

1. applications and affidavits
2. original warrants issued to the ACCC
3. notifications to carriers on the issue and revocation of warrants
4. notifications to other enforcement agencies exercising the authority of an ACCC obtained warrant
5. instruments of delegation and authorisation
6. instruments of revocation
7. evidentiary certificates issued by certifying officers
8. authorisations issued by the Chairman or persons allowed to receive information from a carrier obtained under a warrant
9. a record of how information has been dealt with
10. details of records or information destroyed in accordance with the TIA Act.

Destruction of information or a record obtained under a stored communications warrant

☐ Review information obtained under the warrant on a monthly basis to consider whether it is likely to be required for the purposes for which it can be used under the TIA Act. Relevant considerations will include:

- whether the information obtained is or could be relevant to the investigation
- whether the investigation has been or is being closed
- whether the investigation no longer relates to a serious contravention or serious offence as defined in the TIA Act
- whether retention of the material is required to meet criminal disclosure obligations
- whether retention of the material is required to meet record keeping obligations under the Archives Act.

☐ If you consider that the information is not likely to be required, you must bring this to the attention of the Group General Manager – Enforcement Operations Group immediately.

☐ If the Group General Manager considers that the information is not likely to be required for a permitted purpose, you must make a submission to the Chairman seeking his approval for the destruction. This is done by way of a Minute (using the template provided).

☐ Once the Chairman is satisfied that the information is no longer required, and has signed the destruction approval, the material must be destroyed forthwith.

☐ A copy of both the minute to the Chairman and the minute from the Chairman should be placed in DORIS with access restricted to members of your project team, your office's Evidence Officer and your office's General Manager. Do not proceed to delete or destroy information until you have received the signed approval from the Chairman to do so.

Paper documents

☐ Paper documents need to be shredded and then placed in a secure destruction bin. The original information or record must be destroyed, as well as any working copies made.

Electronic documents

☐ All electronic copies of documents need to be identified. Locations to consider include: DORIS, e-mail, share drives, material available on the Intranet (i.e. Enforcement Committee papers), CDs, DVDs, laptop hard drives and thumb drives.

☐ Once you have identified all electronic documents to be destroyed, you need to e-mail the Director, IT Infrastructure and the Director, IT Governance, who will destroy the information. Your e-mail should:

- confirm that the Chairman has signed the destruction approval minute
- indicate the date by which destruction is requested
- identify each document to be destroyed, for example by providing the:
  - document name
  - TRIM/DORIS number
  - Windows file path and folder name containing the documents (and only those documents)
  - Mailbox/folder containing the relevant document (and only that document)
- cc the Director responsible for the matter and the Deputy General Manager of the E&C Division Executive Office.

☐ For documents stored in other locations, please contact the Director, IT Governance to discuss.

☐ The Director, IT Governance will notify you when destruction has been completed and provide a formal confirmation (nb this is a separate document to the destruction of records form which enforcement staff are required to complete).

☐ The IT Service Desk will arrange for the destruction of all electronic documents **excluding** CDs and DVDs. CDs and DVDs should be shredded by a member of the project team using a shredder. The original information or record must be destroyed, as well as any working copies made.

Secondary documents

- ☐ If material obtained under a stored communications warrant has been extracted and used in either an Enforcement Committee submission or in a Reason to Believe paper, you must identify all copies (both paper and electronic) of these documents.
- ☐ For electronic documents, please ensure there is **one final** version. All duplicate copies should be destroyed following the process for destruction of electronic documents detailed above. To ensure all copies of the document are treated in accordance with this process, you may need to contact other staff members to whom these secondary documents have been provided (whether electronically or in hard copy).
- ☐ In relation to the final version of the secondary documents, the access settings on the DORIS document must be adjusted to restrict access to:
    - members of the project team
    - your office's Evidence Officer
    - your office's General Manager.

  This will ensure that the ACCC meets its obligations under the Archives Act and, if there is any subsequent scrutiny of the ACCC's decision in relation to the matter, the material on which those decisions were based is available for examination.
- ☐ Once you have access-controlled these secondary documents (i.e. Reason to Believe papers or EC papers), please contact the Information Management team, in the IMTS Branch (Helen Goninon and Melissa Smith), who will ensure they are marked for sentencing in accordance with the ACCC's Record Disposal Authority. The Information Management team will provide you with e-mail confirmation that the documents will be sentenced in accordance with the ACCC's Records Disposal Authority.[1]
- ☐ Complete the destruction of records form and store with the original warrant in your office's evidence room
- ☐ Advise the ECD Executive that destruction has taken place.

[1] Enforcement Committee papers are classed as entry 6280 of the ACCC Records Disposal Authority and Reason to Believe Minutes are classed as entry 6292 of the ACCC Records Disposal Authority.

Index of templates

Australian Competition & Consumer Commission

Stored Communications Warrant Record Log

The TIA Act contains a number of reporting requirements designed to ensure that appropriate levels of accountability exist in relation to stored communications warrants. Each year the Attorney-General must prepare and table in Parliament a report setting out certain information relating to stored communications warrants. The TIA Act also provides that the Commonwealth Ombudsman may conduct regular inspections of records and must report to the Attorney-General on the results of those inspections.

The information contained in this record log is used to ensure accurate reporting under the TIA Act.

This document must be used in conjunction with the guidance material **provided in the Enforcement Toolbox on the Intranet. Please be aware that** additional information may be required from you, including details as **to how the information obtained has been dealt with (i.e. how it has been used** within the ACCC and the extent to which it has been communicated **outside the ACCC).**

A. Warrant details

Stored communications warrant number *(Executive office use only)*
TRACKIT
Is this the first warrant application in this matter? If no, how many applications have previously been applied for? (A separate log is required for each application)
Who made the application for the warrant?

What is the document id (i.e. D11/xxx) of the authorisation from the Chairman for them to make the application?	
Who issued the warrant? (Issuing authority)	
Date warrant issued	
Date warrant executed by the carrier (this information will be provided in the Response to a stored communications warrant coversheet)	
Carrier the warrant was given to	
Was the application a telephone application (Yes/No)	
Was the warrant subject to any specific conditions or restrictions? (Yes/No)	
Who received the information from the carrier? What is the document id (i.e. D11/xxx) of the authorisation from the Chairman for them to receive it?	
On what date was the information received? How was the information provided? (i.e. on a	

cd)	
In which evidence room is the information or records obtained by accessing a stored communication stored in? Evidence item number/s	
Have any copies of the information or records been made? If so, where are those copies stored?	
Has the information been referred to or extracted in any secondary material? For example, in EC papers? What is the DORIS ID for those documents?	

B. Maintenance of records

Which evidence room is the original warrant stored in? Evidence item number/s	
Which evidence room are the original application and affidavit stored in? Evidence item number/s	
Which evidence room is the notification to the carrier on the issue (and, if applicable, revocation) of the warrant stored in?	

Evidence item number/s	
Is there a notification to another enforcement agency exercising the authority of an ACCC obtained warrant? (Yes/No) If yes, in which evidence room is the original document stored? Evidence item number/s	
Was there an instrument of revocation? (Yes/No) If yes, in which evidence room is the original stored? Evidence item number/s	
Is there an evidentiary certificate issued by certifying officers? If yes, in which evidence room is it stored? Evidence item number/s	
Were any new authorisations/appointments by the Chairman required? If yes, have they been provided to TPLU in accordance with **their procedures**?	

C. Destruction of records

Has any information obtained under the warrant been destroyed? (Yes/No)	^Under the TIA Act, if the Chairman is satisfied that the information or record obtained by accessing a stored communication is not likely to be required for the purposes for which it can be used under the TIA Act, that information or record must be destroyed. **You must follow the process outlined in the Stored Communications Warrant Checklist, including liaising with the Group General Manager – Enforcement Operations Group and providing a Minute to the Chairman, prior to destroying any such material**^

If no, when was the material last reviewed?	^Information obtained under a warrant must be reviewed each month by the applicant and/or his or her respective branch against the permitted purposes^
If yes, please provide: ▪ the document ID of the Minute to the Chairman recommending destruction ▪ the document ID of the Minute from the Chairman directing staff to destroy information or records	
Where are the details of records or information that has been destroyed stored?	
The document ID of the destruction minute containing relevant details (i.e. date destroyed, method of destruction, copies etc)	

D. Effectiveness of stored communications warrant

Was there an arrest made based on lawfully intercepted information?	
Were there proceedings in which information collected by means of a warrant was given in evidence? If yes: ▪ what are the name of proceedings and the court identifier	

- Commencement date
- Civil or criminal
- Remedies sought
- Finalisation date
- Outcome of proceedings