



AFP National Guideline on data accessed remotely from search premises and third party notifications

Metadata	
Caption	Data accessed remotely from search premises and third party notifications
Document Identifier	ON00007
Description	Details the national standard for managing issues related to police lawfully accessing data that is not physically located at the premises specified in a search warrant and the requirement for third party notifications.
Governance Function	Forensic and Data Centres
Owned by	National Manager Forensic and Data Centres
Date First Approved	18/12/2001 12:00 AM
Contact Person	Coordinator Electronic Evidence
Date Published	18/02/2007 12:00 AM
Date Modified	14/11/2011
Date Last Reviewed	11/10/2011 12:00 AM
Authorised by	National Manager Forensic and Data Centres
Date of Next Review	11/10/2013 12:00 AM
Review Notification	'GovernanceForensics@afp.gov.au'
Instrument Type	National Guideline
Replaces	ON00007-003, ON00008
Stakeholders	AFP Operations
Instrument Classification	UNCLASSIFIED

1. Disclosure and compliance

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

Disclosing any content must comply with Commonwealth law and the [AFP National Guideline on disclosure of information](#).

Compliance

This instrument is part of the AFP's professional standards framework. The [AFP Commissioner's Order on Professional Standards \(CO2\)](#) outlines the expectations for appointees to adhere to the requirements of the framework. Inappropriate departures from the provisions of this instrument may constitute a breach of AFP professional standards and be dealt with under Part V of the [Australian Federal Police Act 1979](#) (Cth).

2. Acronyms

AFP	Australian Federal Police
CFT	Computer Forensics Team
LIMS	Laboratory Information Management
QAR	Quality Assurance Review

3. Definitions

Occupier – for the purposes of this guideline means the premise occupier of the physical search warrant premises.

Remote occupier – for the purposes of this guideline, means the person occupying the remote premises from which data is accessed, and to whom notification will be made (the third party).

4. Guideline authority

This guideline was issued by the National Manager Forensic and Data Centres using power under s. 37(1) of the [Australian Federal Police Act 1979](#) (Cth) as delegated by the Commissioner under s. 69C of the Act.

5. Introduction

This guideline details the national standard for managing issues related to police lawfully accessing data that is not physically located at the premises specified in a search warrant and the requirement for third party notifications. It includes directions on:

- when a third party notification should be made
- the content of notifications
- the manner in which notifications should be made, and
- circumstances where notification is not required.

6. Legislative basis

The framework for administering and managing issues relating to third party notifications about

data accessed remotely from a search premises arises from the requirements of section 3LB of the *Crimes Act 1914* (Cth).

Operating equipment to access data

Section 3L(1) provides that police have authority to operate equipment at a warrant premises to access and copy data. Section 3L(1) further permits access to data that may not be physically located at the warrant premises but is nevertheless believed to contain evidential material as specified in the search warrant. Nothing in section 3LA(1) states that the remote premises must be in Australia and it follows that section 3L(1) can be used to access data wherever it is held.

Whilst section 3K(1) states 'the executing officer may bring to the warrant premises any equipment reasonably necessary for the examination or processing of a thing found at the premises', this section does not specifically state that equipment brought to the premises can be used to access remotely held data.

It is therefore prudent to only **operate equipment already at the premises to access remote data** in order to best safeguard that evidence against any challenge to its admissibility.

Notification

Section 3LB of the *Crimes Act 1914* requires that the executing officer must, if practicable, notify the occupier of the remote premises from which data is accessed when access has occurred.

Further information on the provisions of ss. 3K and 3L is provided in the [Commonwealth Director of Public Prosecutions \(CDPP\) Search Warrant Manual](#).

7. AFP policy

The AFP recognises that developments in information and communications technology have lessened or altogether removed the 'physical' element of many activities. Data constituting evidential material can be stored anywhere on a network, and can usually be accessed from anywhere on that network, regardless of physical location. Searching can be done remotely, breaking the nexus between conducting a search and physically attending at a search site.

Operational requirements must be balanced with the right of remote premise occupiers to be informed when data stored on their premises has been accessed and ensuring that privacy concerns are adequately addressed.

8. Remote access

Increasingly, computers at business premises or even homes are in a networked situation, enabling storage of data at various locations including on the internet. A person can hold their data remotely from their desktop or personal hard drive by, for example:

- storing it in shared drives on a business network or a peer-to-peer network, and/or

connecting to the internet and utilising a file swapping, file hosting or data warehousing service.

Examples include web-based email services e.g. Hotmail, Yahoo or Gmail, where emails are stored on a remote server.

If an executing officer launches a webmail application (intentionally or not), the actions of the executing officer still:

- constitute remote access for the purposes of s 3L(1)
- trigger the notification obligation under s 3LB(1)(b).

9. Identifying remotely held data

It is not always apparent when an officer is searching a computer whether data is held locally or at remote premises.

However, if it appears to an executing officer that he/she is accessing data that is held remotely, the executing officer must take reasonable steps to determine where the data is held. What is reasonable will depend on the circumstances of the case. Options include:

- utilising the assistance of the Computer Forensic Team (CFT)
- use of online tools such as Traceroute, Whois and DNS lookup, and/or
- questioning the premise occupier.

It may not always be possible to identify where the data is being held.

10. When and where to notify

If an address is identified as potentially holding data remotely accessed by police, the notification should be sent to that address, even if it is possible that the data may be stored elsewhere.

Notification must be made as soon as practicable after the data has been accessed.

Where a search warrant is intended to be physically executed on the remote premises, notification about the remote access is still required, and should still be given as soon as practicable. It may not be prudent to provide prior warning of police interest: an option is to provide notification during the execution of the search warrant, at the same time the copy of the search warrant is given.

11. Who notifies

The executing officer of the search warrant is responsible for notification, and for any subsequent contact with the remote occupier.

12. Form and content of notification

The notification proforma provided with this guideline (at Schedule 1) must be used in all instances where notification is made.

The notification must include an appropriate description of what has been accessed and what has been copied, for example individual file names, or descriptors such as:

- all data stored in directory X
- all information associated with account name A and password B.

The notification must include the contact details of the executing officer for the search warrant.

13. Delivery of notification

Whatever method chosen for notification, it should be considered the most appropriate to the circumstances. The notification may be either:

- posted
- emailed
- hand delivered.

Overseas locations still require notification.

14. Recording notification

A copy of the completed notification form (at Schedule 1) should be uploaded into the relevant PROMIS case log.

15. Privacy issues and notification

An executing officer who is contacted by the remote occupier after notification has been made should exercise sound judgement in responding to questions.

Privacy issues relating to the premise occupier must be observed in any discussion with the remote occupier. The executing officer should not disclose any more than is absolutely necessary to give effect to the notice. Disclosure of personal information about a person being investigated should be limited as far as possible.

If necessary, a copy of the original search warrant may be provided to the remote occupier, with all personal identifying information removed e.g. the premise occupier's name and address.

It is reasonable to expect that the remote occupier may have an interest in what offences were being investigated, and in what information was retrieved from his/her system. In responding to these queries, it is appropriate to disclose the offences (quoting the offence name as recorded in the legislation), as well as general information about the types of data retrieved (e.g. image files, word files, databases). However, it is not appropriate to provide an in-depth description of the contents of those files (e.g. child pornography images).

It is also reasonable to expect that some remote occupiers, especially those located overseas, will require further procedural information than those familiar with Australian law.

It is inappropriate to disclose details of police methods or operationally sensitive information.

16. Determining not to notify

The requirement on police is to notify *where practicable*. It is not possible to provide an exhaustive list of circumstances where notification would or would not be practicable, however an executing officer can choose to not notify if, after taking all reasonable steps the following cannot be identified:

- an occupier, or
- an address or contact details for an occupier.

These are likely to be the most commonly encountered situations where notification cannot be provided.

17. Recording of non-notification

When it has been determined that it is not practicable to notify, the decision **must be recorded**.

The non-notification proforma provided with this guideline (at Schedule 2) must be used in such instances. It must include:

- details of the search warrant
- a description of what data was accessed
- the name and AFP number of the executing officer for the search warrant, and
- the reason that notification was not made.

This document should be uploaded into the relevant PROMIS case log.

18. Further advice

Queries about the content of the guideline should be referred to the Coordinator Electronic Evidence, Forensic and Data Centres.

19. References

This guideline should be read in conjunction with relevant operational guidelines and legislation, in particular:

Legislation

- [Australian Federal Police Act 1979](#) (Cth)
- [Crimes Act 1914](#) (Cth)
- [Privacy Act 1988](#) (Cth)

AFP Governance instruments

- [AFP National Guideline on property and exhibits](#)

Other sources

- [Commonwealth Director of Public Prosecutions \(CDPP\) Search Warrant Manual](#)

20. Attachments

[Schedule 1 – Template for Notice under section 3LB of the *Crimes Act 1914* \(Cth\) \(DOC, 50KB\)](#)

[Schedule 2 – Template for Section 3LB of the *Crimes Act 1914*: Record of Non-Notification \(DOC, 50KB\)](#)