Commonwealth
OMBUDSMAN

Report to the Attorney-General on the results of inspections of records under s 55 of the *Surveillance Devices Act 2004*

AUSTRALIAN FEDERAL POLICE
July 2006 to December 2006

SOUTH AUSTRALIA POLICE
July 2005 to June 2006

NEW SOUTH WALES POLICE
December 2004 to December 2006

Report by the Commonwealth Ombudsman
under s 61 of the *Surveillance Devices Act 2004*

August 2007

ISSN 1833-9263

Date of publication: August 2007
Publisher: Commonwealth Ombudsman, Canberra, Australia

Contents

INTRODUCTION

The *Surveillance Devices Act 2004* (the Act) restricts the use, communication and publication of information obtained through the use of surveillance devices, and establishes procedures to obtain permission to use such devices in relation to criminal investigation and the recovery of children. The Act also imposes requirements for the secure storage and destruction of records in connection with surveillance device operations. Section 55(1) of the Act requires the Ombudsman to inspect the records of each law enforcement agency, as defined in s 6(1), to determine the extent of compliance with the Act by the agency and its law enforcement officers.

The term 'law enforcement agency' includes the Australian Crime Commission (ACC), the Australian Federal Police (AFP), the Australian Commission for Law Enforcement Integrity (ACLEI), and specified State and Territory law enforcement agencies (s 6(1)). If any of these agencies utilise the provisions of the Act, the Ombudsman is required to inspect the records relating to that use.

The Ombudsman is also required under s 61 of the Act to report to the Minister at six-monthly intervals on the results of each inspection. In February 2006, it was agreed that the six-monthly intervals should be January to June and July to December each year. Reports to the Minister will include inspections where the results of the inspection have been finalised in the six-month period to which the Minister's report relates. In this context, results are finalised once the Ombudsman's report to the agency is completed.

This report relates to the period 1 January 2007 to 30 June 2007 (the reporting period). In that period, reports on the results of inspections were finalised for the following agencies who used the Act: the AFP, the South Australia Police (SA Police) and the New South Wales Police (NSW Police). Those inspections are summarised below.

Agency	**Period covered by inspection**	**Date of inspection**	**Report to the agency completed**
AFP	January 2006 to September 2006	13–16 November 2006	21 May 2007
AFP	July 2006 to December 2006	16–21 February 2007	21 May 2007
SA Police	July 2005 to June 2006	6 November 2006	29 January 2007
NSW Police	December 2004 to December 2006	7 December 2006 and 12 February 2007	3 May 2007

Detailed reports on the results of each inspection were provided to the relevant agency. This report summarises the significant issues that arose in the inspections and includes the recommendations made to each agency.

CONDUCT OF INSPECTIONS

All records held by each agency that relate to warrants and authorisations issued under the Act during each inspection period were potentially subject to inspection. However, the Ombudsman's discretion under s 55(5) of the Act was exercised to limit the inspections to those warrants and authorisations that had expired or been revoked during the inspection periods. In this report, those records are referred to as 'eligible records'.

The attendance at inspection meetings of the managers of the key areas in the AFP, the SA Police and the NSW Police involved in the administration and application of the Act facilitated the conduct of the inspections.

AUSTRALIAN FEDERAL POLICE

Inspection results determined in the reporting period

The results of two inspections of the AFP's surveillance devices records were determined in the reporting period. The principal inspection was held at the AFP's Telecommunications Interception Division (TID) in Canberra from 16 to 21 February 2007, and examined records from the period 1 July 2006 to 31 December 2006 (the inspection period). Inspecting officers examined a representative sample, inspecting 86 of 172 eligible records (50%). An earlier inspection was also conducted of the AFP's Western Region office in Perth between 13 and 16 November 2006. Surveillance device records from the Perth office for the period January to September 2006 were examined.

A draft report on the results of the inspections was sent to the AFP for comment in March 2007. Comments on the draft report were received on 24 April 2007 and were incorporated into the final report, which was delivered to the AFP on 21 May 2007.

Background

Many improvements in AFP procedures have been noted since the last inspection in August 2006, particularly with respect to the timeliness of reports to the Minister under s 49.

Overall, the records examined were of a high standard, and were generally compliant with the provisions of the Act. However, compliance with s 53 and the maintenance of an appropriate register remained a problem.

Compliance issues

Three compliance issues were identified and one recommendation made as a result of the inspections.

Section 53 register

Section 53 of the Act requires a register of all warrants and authorisations to be kept. The register is to specify the name of the person who issued or refused the application and the date of issue or refusal. If the application is approved the register must also record certain information.

The database utilised by the AFP for the purposes of complying with s 53 did not record refused applications (the database could only record warrants and authorisations that were given a reference number). The database was also deficient in a number of other areas, which led to errors in the recording of issuing officer names and an inability to record information on variations and extensions to warrants.

Recommendation
The Australian Federal Police should, as a matter of priority, implement a register containing information required under s 53 of the *Surveillance Devices Act 2004*. Measures to ensure compliance with s 53 pending the upgrade of the current database should be adopted as soon as possible.

During a visit to the AFP TID premises in August 2007, my staff were shown a new register that would appear to address these concerns. I will advise further on this development in my next report.

Recording 'use' and 'communication'

Under s 52(1)(e) and (f) of the Act, the chief officer of a law enforcement agency is required to record the details of each use within the agency of information obtained by the use of a surveillance device, and each time information obtained by the use of a surveillance device is communicated outside the agency or given in evidence.

The AFP requires investigators to keep 'use and communication' logs in order to fulfil the requirements of s 52. These logs are to be kept contemporaneously to enable investigators to enter details regarding each use and each communication of such information.

While there was an improvement in the number of files containing logs, a number of files inspected did not contain a log, or any other document to fulfil the requirements of s 52. Where logs were present, some did not contain sufficient detail to comply with the record keeping and accountability requirements of the legislation.

The recommendation from the February 2007 report on this issue remains extant.

Content of s 49 reports to the Minister

There was a noted improvement in the timeliness of reports to the Minister under s 49 of the Act. However, the inspection identified two recurring problems.

Section 49(2)(b)(ix) of the Act requires the report to address the benefit to the investigation of the use of the device, and of the general use made or to be made of any evidence or information obtained by the use of the device. This was often not addressed or was addressed in insufficient detail.

Under s 49(2)(b)(iv) of the Act, the report must state the period during which the surveillance device was used. AFP policy defines 'use' as the period from installation to retrieval of a device (or warrant expiry if the device is not retrieved). Despite this guidance, a number of reports continued to identify the period of 'use' of the device, as the whole period of the warrant.

The recommendation from the February 2007 report on this issue remains extant.

Compliance-related issues

Four further issues relating to or having the potential to adversely affect compliance were identified.

Content of affidavits—privacy and other information

An application for a warrant under the Act must be supported by an affidavit setting out the grounds on which the warrant is sought. The application together with the affidavit must contain all of the information to be considered by the issuing officer to enable them to be satisfied that a warrant should be granted (s 16). An application to an appropriate authorising officer for a tracking device authorisation must also contain that information which would be addressed if it were an application for a warrant (s 39).

Applications and supporting affidavits should therefore contain all of the information relevant to the issuing officer's decision whether or not to issue the warrant or the authorisation (ss 16 and 17). There is an implied duty to disclose all relevant information to the issuing officer in the application documents (s 14).

In particular, s 16(2)(c) states that in determining whether to issue a surveillance device warrant, the issuing officer must have regard to the extent to which the privacy of any person is likely to be affected. In order to assist the issuing officer this should be addressed in either the warrant application or supporting affidavit.

A number of files inspected did not comment on the effect on privacy in the application or supporting affidavit. While some affidavits noted the issue of privacy, most did not adequately address the requirement of s 16(2)(c), which would

appear to require an assessment as to the degree privacy will be affected, taking into account the particular circumstances. This issue has been raised in previous reports to the agency.

The applicant should provide all relevant information to allow the issuing officer to make an informed decision on the issue of a warrant or authorisation. This includes information about unusual circumstances.

Installation before authorisation

There was one instance of a device being installed in a package four hours before the appropriate authorising officer had issued the tracking device authorisation. The Attorney-General's Department (AGD) has advised that where the AFP owns a package into which the device is installed, the AFP may install the device before the warrant or authorisation is granted as long as it is not used before the time of issue. However, the AGD noted that there are risks to the admissibility of the evidence obtained in such circumstances. The AFP should be fully cognisant of those risks and manage procedures accordingly.

Templates

In several instances investigators used the template for revoking surveillance device warrants to revoke tracking device authorisations. That template cites the section of the Act relating to the revocation of warrants.

The Act does not provide an express provision to revoke tracking device authorisations, and it is our view that authorisations can be revoked by an appropriate authorising officer using the template in the Commonwealth Director of Public Prosecutions Surveillance Devices manual.

Destructions

When certain conditions have been met, s 46(1)(b) of the Act places an obligation on the chief officer of a law enforcement agency to destroy any record or report comprising protected information held by the agency.

The AFP advised that no destruction of records or information obtained through the use of a surveillance device under this Act had taken place. However, during the inspection TID staff advised that a destruction program was about to begin. The implementation and administration of the destruction program under s 46 will be an area of focus for future inspections.

Best practice and administrative issues

Several matters relating to best practice principles were also noted and discussed with TID staff.

Action sheets

The AFP introduced action sheets as a measure to record actions taken under warrants and authorisations. Where action sheets are completed and placed on file they provide valuable information to the TID and inspecting officers about what has taken place during the course of the warrant or authorisation. However, inspecting officers found that greater detail would enhance the benefits of this initiative.

Initialling all pages of warrants and authorisations

It was again noted that, in most cases, issuing officers did not sign or initial the front page of the warrant or authorisation where the document was more than one page. As previously suggested, appropriate authorising officers, eligible judges and nominated AAT members could be prompted to sign or initial the extra pages by inserting a space for a signature block in the footer of the documents. The AFP has undertaken to ask issuing officers to initial every page of a warrant or authorisation.

Regional inspection—Perth

In November 2006, inspecting officers examined surveillance devices records from the AFP Western region for the period January to September 2006.

In general, inspecting officers found that the documents from the Western region in support of applications for surveillance device warrants and authorisations were satisfactory. However, some deficiencies in record keeping were identified and were discussed with the Special Project Registrar, investigators and managers during, and at the conclusion of, the inspection.

Compliance and best practice issues arising from this inspection have been included in the results reported above. However, some additional matters were of note:

- two original affidavits from the Western region were misplaced (one was found in the Perth office during the inspection but the other was unable to be located)
- the timeliness of Final Effectiveness Reports (FERs) and s 49 reports to the Minister.

The inspection of AFP records for the period 1 July to 31 December 2006, which was undertaken at the TID from 16 to 21 February 2007, showed an improvement in the general level of documentation and in the overall standard of records from the Western region, most particularly in the timeliness of FERs and the inclusion of a statement to address the issue of privacy in supporting affidavits.

SOUTH AUSTRALIA POLICE

Inspection results determined in the reporting period

The results of the first inspection of the South Australia Police's (SA Police) surveillance devices records were finalised in the reporting period. The inspection was conducted at the SA Police Telecommunications Interception Section (TIS) and the office of the Special Intelligence Section (SIS) Telecommunications Interception Division (TID) in Adelaide.

The inspection took place on 6 November 2006 and examined records from the period 1 July 2005 to 30 June 2006 (the inspection period). Inspecting officers examined 100% of the SA Police's eligible records.

A draft report on the results of the inspection was sent to the SA Police for comment in December 2006. Comments on the draft report were received in January 2007 and were incorporated into the final report, which was delivered to the SA Police on 29 January 2007.

Background

In determining the extent of compliance by the SA Police and law enforcement officers of the SA Police with the Act, this office was mindful of the challenges faced by the SA Police in settling its procedures after the commencement of the Act. It was noted that this was the first inspection of the records of the SA Police pursuant to the Act. Overall, the records kept by TIS and SIS under the Act were of a high standard, and were generally compliant with the provisions of the Act.

Compliance issues

Three compliance issues were identified and a recommendation was made in regard to each issue.

Content of s 49 reports to the Minister

A report on each warrant or authorisation must, as soon as practicable after the warrant or authorisation ceases to be in force, be provided to the Minister. Section 49(2) of the Act sets out the details to be included in the report in order for the Minister to be informed of the use by law enforcement agencies of surveillance devices. The inspection found that the relevant details were not contained in the s 49 reports for the Minister. It was also not clear from the file that copies of warrants, authorisations and revocations had been sent to the Minister as required by s 49(1)(e). It is important that the SA Police record, for internal and external audit purposes, whether the documents have been sent.

This office advised the SA Police to send an addendum to the Minister correcting the current deficient reports to ensure that the SA Police were compliant with the Act.

Where it is thought that a warrant would be invalid if challenged, a s 49 report is still required. If the warrant has not been executed the report will note as much and go no further.

Recommendation
The SA Police should ensure that the report sent to the Minister under s 49(1) of the Act includes all the information required by s 49(2).

The SA Police have advised that the s 49 reports have been resubmitted to include necessary information.

Timeframe for revocation of warrants

The revocation of a warrant does not come into effect until an instrument of revocation has been signed by a person authorised to revoke a warrant. A notice of intention to revoke, or the cessation of use of a device, does not constitute the revocation of a warrant. Nor can a revocation be made orally.

In two instances, the instrument of revocation was not signed until after the warrant had expired. There was no evidence to indicate when the revocation request was submitted. One instrument of revocation was signed 27 days after the original expiry date, while the other instrument of revocation was signed 78 days after the expiry of the warrant. As the warrants had expired, there was no longer any warrant to revoke and thus the revocations were ineffective.

As the need for the warrants had ceased before the expiry date, it was both appropriate and a requirement of the Act that each warrant be revoked (s 20(2)). Although the revocations were not made in time, we note that the SA Police discontinued use of the devices once they ceased to be necessary for obtaining evidence, as required by s 21(2).

Recommendation
The SA Police should ensure that once the need for a surveillance device ceases all revocations are promptly signed by an appropriate officer.

The SA Police advised that the responsibility for managing all reporting aspects of warrants and authorisations and the revocation of warrants will now rest with the Officer in Charge, TIS, and not the area responsible for executing the warrant. Central control of the reporting and revocation requirements of the Act should ensure this requirement is complied with.

Delegation of power to revoke warrants

Section 20 of the Act provides that the chief officer may revoke warrants in certain circumstances. Under s 63 of the Act the chief officer may, by writing, delegate to

a member of staff of the agency who is an SES employee or a person of equivalent rank, all or any of the chief officer's powers or functions, including the power to revoke surveillance device warrants.

The inspection team found that an Assistant Commissioner had, without proper authority, signed the four instruments of revocation inspected. As no written delegation was executed, the Assistant Commissioner did not have power to revoke a warrant and any revocation which might otherwise have been valid would have been ineffective.

Recommendation
The SA Police should ensure that an instrument of delegation is signed by the Commissioner as chief officer under s 63 of the Act to authorise persons of appropriate rank to exercise the Commissioner's powers and functions under the Act.

The SA Police advised that an instrument of delegation was signed by the Commissioner on 27 November 2006 authorising the Assistant Commissioner Crime Service to exercise powers under the Act.

Best practice and administrative issues

Several matters relating to best practice principles were also noted. These included:

- The records required for the inspection were held across three separate units of the SA Police. The dispersed material may become difficult to administer if the provisions of the Act are utilised more widely by the SA Police.
- 'Action sheets' are used by other law enforcement agencies as an administrative record of actions taken under an executed warrant. The SA Police should consider implementing a similar practice.
- The template for an application for a surveillance device warrant incorrectly refers to s 16 as the power for making the application. Section 16 is the provision under which a warrant is issued, while s 14 gives the right to make an application for a warrant.
- The reports to the Minister under s 49 must be provided 'as soon as practicable' after the warrant or authorisation 'ceases to be in force'. It has been agreed with other law enforcement agencies that two months from the date of expiry or revocation of a warrant or authorisation would be a reasonable timeframe for provision of the reports to the Minister. If this timeframe cannot be met, a note detailing the reasons is placed on file. Assuming the reasons to be sound, this would in our opinion satisfy the

requirement to provide the report 'as soon as practicable'. The SA Police may wish to adopt a similar practice.

- It was noted that it is the practice to obtain fresh warrants and authorisations rather than seeking an extension or a variation, even though the latter options may be available. If new warrants or tracking device authorisations are obtained, they should refer to the previous warrants or authorisations for the installation and use of the devices. While the issue of a new warrant is not prohibited under the Act, it may be simpler to utilise the provisions for an extension or variation.
- The quality of the affidavits was of a high standard. The effect on privacy and the evaluation of alternative means of obtaining evidence was addressed thoroughly and thoughtfully, in accordance with the intent of the Act. While 'the likely evidence or intelligence value of any evidence or information sought to be obtained' was not overlooked, it would be helpful if this issue were also dealt with under its own heading in the affidavit.

NEW SOUTH WALES POLICE

Inspection results determined in the reporting period

The results of the first inspection of the New South Wales Police (NSW Police) records covering the period from 15 December 2004 to 31 December 2006 (the inspection period) were finalised in the reporting period.

The inspection was carried out at the NSW Police's Counter Terrorist Co-ordination Command (CTCC)[1] on 7 December 2006, and again on 12 February 2007. The draft report was sent to the NSW Police in March and a response was received in April 2007.

The NSW Police was the first state law enforcement agency to use the Act, obtaining warrants from January 2005, a month after the Act came into force. Owing to the relatively low number of warrants and authorisations in the inspection period, inspecting officers examined 100% of the eligible records.

Background

Although this report contains the results of the first inspection of the records under the Act, the NSW Police has used the provisions of the Act for an extended period. In the opinion of this office, sufficient time had elapsed for the NSW Police to

[1] From 1 March 2007 the CTCC became known as the Anti-Terrorism and Security Group, part of the Counter Terrorism and Special Tactics Command. As this change took place after both inspections and the inspection period, this report continues to refer to the CTCC.

establish procedures to ensure compliance with the Act. While the standard of affidavits supporting warrant applications was particularly high, overall the NSW Police was not compliant with the Act for the period covered by the records inspected, and did not have adequate procedures and policies in place to ensure compliance in the future.

Compliance issues

Three compliance issues were identified resulting in two recommendations.

Recording use and communication under s 52

Under s 52 of the Act, the chief officer of a law enforcement agency must cause to be kept, among other things, details of each:

- use by the agency, or by a law enforcement officer of the agency, of information obtained by the use of a surveillance device by a law enforcement officer of the agency
- communication by a law enforcement officer of the agency to a person other than a law enforcement officer of the agency, of information obtained by the use of a surveillance device by a law enforcement officer of the agency
- occasion when, to the knowledge of the law enforcement officer of the agency, information obtained by the use of a surveillance device was given in evidence in a relevant proceeding.

Details of each 'use' of information include the use of the information within the agency to further the investigation. Details of each 'communication' of information refers to the communication of information to a person other than a law enforcement officer of the agency. The statements do not adequately meet the requirements of s 52.

Recommendation
NSW Police should take action to ensure full compliance with the requirements of s 52 of the *Surveillance Devices Act 2004*.

The NSW Police agreed that further records needed to be kept in relation to use and communication under s 52 of the Act.

List of previous warrant applications

Under s 16(2)(f) of the Act, in determining whether a surveillance device warrant should be issued, the issuing officer must have regard to any previous warrant sought or issued under the Act in connection with the same alleged offence or the same recovery order.

The NSW Police included in its affidavits all previous warrant applications under the *Listening Devices Act 1984* (NSW), but omitted to include any previous warrants applied for and granted under the Surveillance Devices Act. Most of the surveillance device warrants issued under the Act to the NSW Police related to ongoing investigations where previous warrants had been sought and granted.

Although not required by the legislation to be included in the supporting affidavit, this is the most appropriate place for the information on previous applications or warrants to be recorded. Applications for warrants under other legislation but relating to the operation are not required, but may also be included for the information of the issuing officer. However, they should be clearly identified as relating to the operation overall, and not as previously issued warrants under this division of the Act.

The NSW Police has advised that the legislative requirements surrounding the making of an application for a warrant, including this issue, will be addressed in relevant guidelines.

Reports to the Minister under s 49

Section 49 of the Act requires the chief officer of a law enforcement agency to provide reports to the Minister on each warrant and authorisation issued under the Act. The reports must be provided 'as soon as practicable' after the warrant or authorisation 'ceases to be in force'. The chief officer must also provide the Minister with a copy of each warrant and authorisation, and any instrument revoking, extending or varying the warrant. At the time of the inspections in December 2006 and February 2007, the NSW Police had not reported to the Minister on any of the warrants obtained under the Act.

In addition to the reports to the Minister, the chief officer of a law enforcement agency is also to submit an annual report to the Minister under s 50 of the Act, for the preceding financial year period. The annual report is to be sent in addition to the reports under s 49.

Recommendation
The NSW Police should ensure that reports to the Minister on each warrant and authorisation issued or given under the *Surveillance Devices Act 2004* are provided as soon as practicable after the warrants or authorisations cease, as required by s 49 of that Act.

The NSW Police has advised that the reports under s 49, in relation to warrants previously obtained, had been compiled prior to the Ombudsman's inspection. However, the Ombudsman's representative indicated that these reports did not contain sufficient detail. Accordingly those reports were withheld and amended reports were drafted and will be forwarded to the Minister in due course. The

requirements for submission of reports under s 49 will be included in relevant guidelines.

Additionally, the Terrorism Investigation Squad has established a Command Management Framework (CMF) portfolio specifically relating to applications and record keeping under the Act. The CMF, a review and evaluation tool, will operate on a monthly reporting cycle. Delegation processes are also being streamlined to enable appropriate delegation of authority in respect to s 49 reports.

Best practice and administrative issues

Several matters relating to best practice principles were also noted. These included:

- The template for an application for a surveillance device warrant incorrectly refers to s 16 as the power for making the application. Section 16 is the provision under which a warrant is issued, while s 14 gives the right to make an application for a warrant.
- Section 49 reports to the Minister must state the period during which a surveillance device was 'used'. To ensure that the Minister is comprehensively informed, and to avoid confusion over the interpretation of 'use', it would be preferable for the report to state the date the device was installed and the date it was retrieved, as well as any period during which the device was activated.
- Warrants that are more than one page in length should be initialled on the first and any subsequent pages that do not contain the issuing officer's signature.

Prof. John McMillan
Commonwealth Ombudsman