Commonwealth OMBUDSMAN

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

AUSTRALIAN CRIME COMMISSION
1 January 2007 to 30 June 2007

NEW SOUTH WALES POLICE
1 January 2007 to 30 June 2007

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

August 2008

ISSN 1833-9263

Date of publication: August 2008
Publisher: Commonwealth Ombudsman, Canberra, Australia

OR

Requests and enquiries can be directed to the Director Public Affairs,
Commonwealth Ombudsman, GPO Box 442, Canberra ACT 2601;
email ombudsman@ombudsman.gov.au.

This report is available online from the Commonwealth Ombudsman's website
at http://www.ombudsman.gov.au.

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 between this office and the Attorney-General's Department (AGD) 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 ACC and the New South Wales Police (NSW Police). Details on those inspections are provided below.

Agency	Period covered by inspection	Date of inspection	Report to the agency completed
ACC	1 January 2007 to 30 June 2007	3 to 6 September 2007	25 January 2008
NSW Police	1 January 2007 to 30 June 2007	31 October 2007 to 2 November 2007	22 April 2008

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

CONDUCT OF INSPECTIONS

All records held by an agency that relate to warrants and authorisations issued under the Act during the 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'.

Both the ACC and NSW Police provided every assistance in the conduct of the inspections. The importance they place on compliance with the Act and their efforts to implement the recommendations made by this office should be noted.

AUSTRALIAN CRIME COMMISSION

Inspection results determined in the reporting period

The report of one inspection of the ACC's surveillance devices records was finalised in the reporting period. The inspection was conducted at the ACC's Electronic Product Management Centre (EPMC) in Sydney from 3 September to 6 September 2007, and examined records from the period 1 January 2007 to 30 June 2007. This office examined 100% of the ACC's eligible records. A final report was provided to the ACC on 25 January 2008.

Background

Based on an assessment of 42 eligible records for surveillance devices warrants and authorisations, the ACC was assessed as being generally compliant with the Act. However, a number of compliance and best practice issues were identified as a result of the inspection.

Overall, the records for warrants and authorisations were of a high standard. However, six recommendations were made, relating to three compliance issues and three best practice issues.

In addition, some key initiatives of the ACC to improve compliance with the Act were recognised.

The ACC advised that it had not used the surveillance device laws of any State or Territory during the inspection period. Therefore, the Ombudsman was not required to undertake an inspection of ACC records under s 55(2) of the Act during this inspection period.

ACC initiatives

Since the Act came into force, the ACC has introduced several procedures and further training to assist ACC investigators and administrative staff in complying with the Act. The ACC has also advised that a mandatory compliance training program in relation to compliance with the Act will be introduced in 2008 for all ACC operational staff. The training will address statutory reporting requirements, recommendations and best practice issues identified by this office.

Destructions

This was the first inspection period in which the ACC had destroyed any records relating to the use of a surveillance device, and therefore, the first inspection of this process and legislative requirement. Section 46 makes provisions for dealing with records obtained by use of surveillance devices, and s 46(1)(b) details the requirements for the destruction of these records.

The ACC had destroyed records and reports held in regional offices comprising protected information associated with two warrants. For each warrant for which protected information was destroyed, there was a certification by the chief officer of the ACC that the protected information was no longer required, and the destructions occurred within five years after the making of the record or report.

Compliance issues

Three recommendations were made relating to issues of compliance.

Late reports to the Minister

Under s 49 of the Act, the chief officer of the law enforcement agency must make a report to the Minister as soon as practicable after a warrant or authority ceases to be in force. The Minister is to be provided with copies of the warrant or authorisation and of any instrument revoking, extending or varying such a warrant or authorisation.

Although the Act does not define ‘as soon as practicable’, it was previously agreed between this office and the ACC that three months from the cessation of the warrant or authorisation would be an acceptable period within which to make the report. Several reports were outside this time frame and while some of these reports were delayed due to operational circumstances, not all the late reports included any justification. The ACC advised that they would be more closely monitoring compliance with this reporting requirement.

For several files, it also appears that the reports did not contain all the relevant documentation, as required by the Act.

Recommendation

The Australian Crime Commission should ensure that s 49 reports to the Minister are sent as soon as practicable (within three months, unless there are special circumstances) after the warrant or authorisation ceases to be in force, and that these reports include all relevant documentation.

Retrieval of a device after expiry of authorisation

Section 22(1) of the Act makes provision for a law enforcement officer to apply for the issue of a retrieval warrant in respect of a surveillance device that was lawfully installed under a warrant or tracking device authorisation, if the law enforcement officer suspects on reasonable grounds that the device is still installed (after expiry of the warrant or authorisation).

One tracking device, lawfully installed under a 30-day tracking device authorisation, was retrieved five days after expiry of the authorisation. The ACC advised that due to failure of the device they were unable to locate and retrieve it before the authorisation expired and that a retrieval warrant had not been subsequently sought as there was a misunderstanding over the date the authorisation expired.

Recommendation

The Australian Crime Commission should ensure that retrieval of surveillance devices is carried out in accordance with the provisions of the *Surveillance Devices Act 2004*, and where necessary, obtain a retrieval warrant under ss 22–26 of the Act if the authorisation for the installation has expired before the device is retrieved.

Use of subsequent devices and reporting requirements

During one operation, a composite listening and tracking device was installed. The device had been authorised by two separate warrants, one authorising the listening device and the other authorising the tracking device. The ACC advised the Minister under s 49 of the Act that the listening device warrant had been executed, but that the original tracking device warrant had not been executed. Once the composite device was installed, both warrants had been executed.

These warrants expired and a subsequent warrant was issued to authorise continued use of the tracking device. Product was obtained from the tracking device under the second warrant and this led to an arrest. The ACC advises that no listening product was obtained from the composite device during this later period.

Although it does not appear that any product was unlawfully obtained, and that the error was limited to reporting requirements under s 49 of the Act, the use of a composite device under separate warrants authorising the use of the component devices has the potential to create confusion, which could readily lead to unlawful surveillance. It is noted that the ACC have provided the Minister with an amending report under s 49 report of the Act.

Recommendation

The Australian Crime Commission should review administrative practices to ensure the accuracy of s 49 reports to the Minister, and recordkeeping practices as required by s 52 of the Act. In addition, when using composite devices, if the operation allows it, the Chief Executive Officer should consider the appropriateness of obtaining one warrant for all surveillance capabilities.

Best practice and administrative issues

Three recommendations were made relating to best practice and administrative issues.

Section 16(2)(c)—Privacy

Section 16(2) of the Act sets out those matters that an eligible Judge or a nominated AAT member as issuing officer must have regard to in determining whether to issue a surveillance device warrant. One of those matters is 'the extent to which the privacy of any person is likely to be affected' (s 16(2)(c)).

Although there is no provision in the Act that requires the ACC to state in a warrant application the extent to which the privacy of any person is likely to be affected—and the lack of such information does not therefore go to the issue of compliance, nor will it necessarily affect the validity of a warrant—as a matter of best practice the issuing officer will be assisted by information in the application that addresses the circumstances in which the device will be used as it relates to privacy.

The inspection found that the majority of the warrant applications mentioned privacy. This is a significant improvement over past inspections. However, in only a minority of applications was privacy addressed in a manner or in sufficient detail to be of any real assistance to an issuing officer.

The ACC advised in January 2008 that the need to satisfy statutory requirements for a warrant to be issued, including privacy, continues to be a central focus of national compliance training for relevant staff.

Recommendation

The Australian Crime Commission should ensure that all warrant applications include information on the extent to which the privacy of any person is likely to be affected by the use of a surveillance device, so that issuing officers can more readily address the requirements of s 16(2)(c).

Timeliness of revocations of warrants assessed as no longer necessary

Sections 20 and 21 of the Act require the chief officer of the ACC to revoke a warrant by instrument in writing if a law enforcement officer, to whom the warrant was issued, is satisfied that the use of a surveillance device under the warrant is no longer necessary. The law enforcement officer must immediately notify the chief executive officer that the use of the surveillance device is no longer necessary. After revoking a warrant, the chief officer must take steps to ensure that use of the surveillance device is discontinued.

Although only a small number of warrants were revoked, three of these warrants were revoked after the warrants had expired. One warrant was revoked 15 days after expiry, and two warrants were revoked 25 days after expiry. In two of the three cases, the notification from the law enforcement officer was signed three weeks before the warrants expired. These cases suggest that internal procedures for ensuring compliance with the Act in terms of revocation of warrants, and the discontinuance of the use of surveillance devices under warrants, needs some attention to ensure compliance with the provisions of ss 20 and 21 of the Act.

The ACC advised that a new procedure will be introduced to ensure that the Chief Executive Officer's office is alerted to the urgency in relation to the revocation of surveillance devices warrants.

Recommendation

The Australian Crime Commission should review internal procedures relating to the revocation of warrants assessed as no longer necessary, and the discontinuance of the use of surveillance devices after revocation of a warrant, to ensure compliance with ss 20 and 21 of the Act.

Initialling warrants and authorisations

The initialling of warrants and authorisations is an issue of best practice, to ensure the authenticity of the documents. Many warrants and tracking device authorisations were not initialled on the front page when the warrant was longer than one page.

As a matter of best practice, warrants and authorisations should be initialled on all pages as well as signed on the final page. This will ensure that all parties can be satisfied that the pages of the warrant or authorisation are original pages and were properly authorised.

This office accepts that the ACC cannot require an AAT member or an eligible judge to initial all pages. However, use of a prompt on the first page as a footnote would not depart from the prescribed form and may solve this problem.

Recommendation

The Australian Crime Commission should continue to work with issuing officers (eligible judges, nominated AAT members and appropriate authorising officers) to ensure that they initial the pages of warrants and authorisations that do not contain their signature. Consideration should be given to the use of a prompt on the first page as a footnote.

NEW SOUTH WALES POLICE

Inspection results determined in the reporting period

The results of the second inspection of the New South Wales Police (NSW Police) records covering the period from 1 January to 30 June 2007 were finalised in the reporting period.

The inspection was held at the office of the NSW Police Anti-Terrorism Group in Sydney from 31 October to 2 November 2007 and examined 100% of eligible records. A final report was provided to the NSW Police on 22 April 2008.

Background

Based on an assessment of 33 eligible records for surveillance devices warrants and authorisations, NSW Police is assessed as generally compliant with the provisions of the Act. Overall, the records examined were of a high standard. However, a number of compliance and best practice and administrative issues were identified as a result of the inspection.

Three compliance issues were identified and five best practice and administrative issues were noted. NSW Police advised in February 2008 that they are committed to continuous improvement in relation to these compliance and best practice and administrative issues, and have already implemented new standard operating procedures and training to ensure improvement in these areas.

The new Standard Operating Procedures (SOPs) provide policy and procedural advice to investigators on the operational aspects of the Act. They address some of the issues raised in the last inspection report, for example: the content of s 49

reports to the Minister and submission requirements; recording use and communication of protected information under s 52 of the Act; and listing previous surveillance device warrants in applications for warrants for the same alleged offences. It is also noted that NSW Police has, since receiving the inspection report, revised the SOPs to address some of the recommendations made in the report.

In a positive step, NSW Police has developed and implemented a new Command Management Framework (CMF) specifically to monitor surveillance devices warrants and reporting requirements under the Act in order to ensure compliance.

Compliance issues

Late reports to the Minister

Under s 49 of the Act, the chief officer of the law enforcement agency must make a report to the Minister as soon as practicable after a warrant or authority ceases to be in force. The Minister is to be provided with copies of the warrant or authorisation and of any instrument revoking, extending or varying such a warrant or authorisation.

In the previous inspection report to the agency in May 2007, the Acting Ombudsman recommended that:

> 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 under s 49 of the Act.

Although the Act does not define 'as soon as practicable', it was previously agreed between this office and NSW Police that three months from the cessation of the warrant or authorisation would be an acceptable period within which to make the report. The majority of the reports inspected were sent to the Minister outside of this time frame. The reason for the late submission of many of the reports appears to have been due to organisational issues, rather than special circumstances. NSW Police advised that they would be more closely monitoring compliance with this reporting requirement.

Additionally, incorrect information was provided to the Minister in some of the reports. NSW Police identified this mistake before the inspection and advised that these reports were being corrected. NSW Police provided the revised reports to the Minister in February 2008.

Recommendation

NSW Police should ensure that s 49 reports to the Minister are sent as soon as practicable (within three months, unless there are special circumstances) after the warrant ceases to be in force. Furthermore, greater attention to detail needs to be given to ensure the accuracy of all information in these reports, particularly in relation to whether or not the warrants have been executed.

Citation of relevant offences in warrant applications and warrants

Section 17(1)(b)(ii) of the Act requires that a surveillance device warrant specify the alleged relevant offence(s) in respect of which the warrant was issued. Several of the warrants did not specify the section number and title of the Act under which the relevant offences were prescribed.

Although there is no provision in the Act that requires NSW Police to state in a warrant application the specific details of the relevant offence, s 14(1) of the Act states that a law enforcement officer may apply for the issue of a warrant if the officer suspects that a relevant offence has been, is being, is about to be, or is likely to be committed.

Full details of the relevant offence(s), including section numbers and titles of Acts, need to be provided by NSW Police in the application for a warrant so that the issuing member can in turn ensure the warrant contains details of the relevant offences, as required under s 17(1)(b)(ii) of the Act.

Recommendation

NSW Police should ensure that warrant applications provide full details of the relevant offence(s) including the section number and title of the Act, so that issuing officers can ensure that the warrant meets the requirements of s 17(b)(ii) of the Act.

Recording 'use' and 'communication'

Under ss 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 from the surveillance device, and each communication outside the agency of information obtained from the surveillance device. For most of the files it was noted that there was no register recording this information.

As the NSW Police and the AFP are regularly sharing information regarding joint operations, this presents some challenges for record keeping in relation to the requirements of s 52 of the Act. It is also noted that there are concerns from NSW Police that s 52 of the Act does not make adequate provision for fast moving and

fluid joint investigations involving external partner law enforcement or intelligence agencies and that legislative reform may be necessary to address this issue. In the absence of any legislative change, it may be beneficial for NSW Police to liaise with other law enforcement agencies to share methods and strategies for complying with these provisions.

Recommendation

NSW Police should ensure that records are kept, as required under s 52(1)(f) of the Act, detailing each communication of 'protected information' obtained from a surveillance device, to a person external to the agency, including external agencies involved in joint operations with NSW Police. The records kept should be detailed in the 'Communication of information' form (register), as set out in NSW Police Standard Operating Procedures.

Best practice and administrative issues

Section 16(2)(c)—Privacy

Section 16(2) of the Act sets out those matters that an eligible Judge or a nominated AAT member as issuing officer must have regard to in determining whether to issue a surveillance device warrant. One of those matters is 'the extent to which the privacy of any person is likely to be affected' (s 16(2)(c)).

The use of a surveillance device may, in the circumstances, be highly intrusive, and the extent to which that person's privacy will be affected may be great. In other circumstances, the extent to which a person's privacy will be affected may be minimal in comparison. The affidavit should, as a matter of best practice, give the issuing officer an idea of the reality of what is likely to be seen or heard from use of the device.

Although most warrant applications made reference to the effect the surveillance device would have on privacy, there was a general lack of detail, and some of the applications did not make any reference to privacy.

As the new SOPs provide guidance to investigators to ensure that sufficient material is provided in affidavits for warrants, it is expected that the issue of privacy will be better addressed in affidavits in the future.

Recommendation

NSW Police should ensure that all warrant applications include information on the extent to which the privacy of any person is likely to be affected by the use of a surveillance device, so that issuing officers can more readily address the requirements of s 16(2)(c).

Listing 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. Although the legislation does not require the warrant application to include the previous warrants sought under the Act, the application is the most appropriate place for this information.

Many of the warrant applications did not include the details of all previous surveillance devices warrants sought for the same alleged offences. While some warrants listed details for some of the previous warrants, there were previous and connected surveillance devices warrants that were still current that were not listed.

It is noted that the new SOPs address this issue and state that NSW Police must provide in applications for surveillance devices warrants the details of any previous warrants issued under the Act in connection with the same alleged offence.

Recommendation

NSW Police should ensure that warrant applications provide full details of any previous related warrants under the Act, so that issuing officers can more readily meet the requirements under s 16(2)(f) of the Act.

Relevant offences

A State or Territory law enforcement officer may apply for the issue of a surveillance device warrant if they suspect on reasonable grounds that one or more relevant offences have been, are being, are about to be, or are likely to be, committed (s 14(1)(a)). A relevant offence is a Commonwealth offence (s 14(2) and s 6(1)) rather than a State offence.

Several of the warrants and associated applications inspected included state offences in addition to the relevant Commonwealth offences. As the warrant was issued for a relevant Commonwealth offence, the inclusion of State offences is not an issue of compliance, but rather one of best practice.

It is noted that NSW Police have developed and implemented new SOPs and that these specifically advise staff that NSW Police cannot obtain a surveillance devices warrant for a State offence. The SOPs should also include advice that State offences should not be listed alongside Commonwealth offences when making such an application. Such a practice would help to avoid the possibility of an application being raised without a relevant Commonwealth offence being listed.

Initialling warrants and authorisations

The initialling of warrants and authorisations is an issue of best practice, to ensure the authenticity of the documents. Many warrants and tracking device authorisations were not initialled on the front page when the warrant was more than one page (and signed on the last page). It is accepted that NSW Police cannot require an AAT member or an eligible judge to initial all pages. However, use of a prompt on the first page as a footnote would not depart from the prescribed form and may solve this problem.

Recommendation

NSW Police should continue to work with issuing officers (eligible judges, nominated AAT members and appropriate authorising officers) to ensure that they initial the pages of warrants and authorisations that do not contain their signature. Consideration should be given to the use of a prompt on the first page as a footnote.

Prof. John McMillan
Commonwealth Ombudsman