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 July 2007 to 31 December 2007

AUSTRALIAN FEDERAL POLICE
1 July 2007 to 31 December 2007

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

March 2009

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 July 2007 to 31 December 2007

AUSTRALIAN FEDERAL POLICE
1 July 2007 to 31 December 2007

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

March 2009

ISSN 1833-9263

Date of publication: March 2009
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 a child under a 'recovery order' (as defined by the Act). 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 July 2008 to 31 December 2008 (the reporting period). In that period, reports on the results of inspections were finalised for the ACC and the AFP. Details on those inspections are provided below.

Agency	Period covered by inspection	Date of inspection	Report to the agency completed
ACC	1 July 2007 to 31 December 2007	11 to 14 March 2008	October 2008
AFP	1 July 2007 to 31 December 2007	31 March to 4 April 2008	October 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 AFP cooperated fully 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.

The Ombudsman must also inspect the records relating to the use by the ACC of surveillance devices under the law of a state or territory in accordance with s 55(2) of the Act. The ACC advised that it had not used a surveillance device under the laws of a state or territory during the inspection period.

AUSTRALIAN CRIME COMMISSION

Inspection results

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 11 to 14 March 2008, and examined records from the period 1 July 2007 to 31 December 2007. This office examined 100% of the ACC's eligible records. A final report was provided to the ACC on 15 October 2008.

Based on an assessment of 55 eligible records for surveillance devices warrants and authorisations and one destruction record, the ACC was assessed as generally compliant with the Act. Overall, the records examined were of a high standard. However, four recommendations were made, relating to two compliance issues and two administrative issues.

The inspection noted that the ACC had been keeping more detailed records of use and communication of information obtained from a surveillance device, as required by s 52 of the Act. It also noted improvements in providing copies of warrants and authorisations to the Minister, as required under s 49 of the Act.

A subsequent inspection was conducted in September 2008. The results of this inspection are yet to be finalised and are not included in this report.

Compliance issues

Two recommendations were made relating to issues of compliance.

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. Of 45 relevant files inspected, three s 49 reports had not been completed. Another 21 files did not contain any documentation showing that a report had been sent to the Minister. The latter issue is problematic in that this office cannot confirm that the reports were sent and the ACC did not have a clear audit trail to verify this fact itself.

Of the remaining files containing documentation demonstrating that a report had been sent, nine of these reports were sent later than three months after the warrants ceased.

The ACC advised that the centralisation of the surveillance devices administration within its EPMC would improve timeliness, and that improvements had been made in recording the fact that a report has been sent to the Minister and also in retaining file copies of reports.

Section 49 sets out the information that must be included in the report to the Minister. Overall, the standard of compliance was good in this regard. However, some issues were noted.

Section 49(2)(b)(iv) provides that the report must state the period during which the device was used. There was one instance of information being obtained after a warrant had expired, and incorrect information consequently being provided to the Minister. This has since been corrected.

Section 49(2)(b)(ii) provides that the report must state the name of each person involved in the installation and maintenance or retrieval of the surveillance device. In four cases, it appeared that technical staff from the Western Australia (WA) Police and possibly the WA Crime and Corruption

Commission (WACC) assisted the ACC with the installation of surveillance devices. WA Police and possibly the WACC provided code numbers for those persons involved and it appears they declined to provide names. The ACC noted the concern of this office that the Act requires names, and amended reports were forwarded to the Minister with correct details.

The following recommendation was made:

Recommendation

The Australian Crime Commission should ensure that s 49 reports to the Minister are sent as soon as practicable (within three months) after the warrant or authorisation ceases to be in force, that a record is kept of the date that the reports are sent, and that all of the reports contain complete and accurate information.

Other issues

There was one instance identified of a device being used and product being obtained after the warrant had expired. The device had a listening component and a tracking component. The listening component ceased to be active when the warrant expired, but the tracking component remained active due to an oversight. The tracking data obtained after expiry of the warrant was stored with restrictions prohibiting access for investigative and/or related purposes.

Section 17 of the Act details the information required to be recorded on a surveillance device warrant. Two warrants did not specify the name of the applicant as required by s 17(b)(i). In addition, there were two warrants where it was unclear who had issued the warrant and one extension where it was unclear who had granted the extension. These names are required to be written on the warrant (s 17(3)). The ACC noted the problem and advised that it will continue to work with issuing officers to ensure compliance with s 17 of the Act.

Recommendation

The Australian Crime Commission should ensure that warrants contain all the required information as prescribed by s 17 of the Act. In addition, when warrants are extended, the Australian Crime Commission should continue to work with issuing officers (eligible judges and nominated AAT members) to ensure that the issuing officers comply with s 17(3) of the Act, by printing their name on the warrant.

Destructions

This was only the second inspection in which the ACC had destroyed records relating to the use of a surveillance device. Section 46 makes provision 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 one relevant file that had been held in the Brisbane office. This destruction occurred in accordance with the relevant legislative provisions.

Administrative issues

Two recommendations were made to improve administration in relation to the Act.

Privacy

Section 16(2)(c) of the Act states that an issuing officer (an eligible judge or AAT member) must have regard to 'the extent to which the privacy of any person is likely to be affected' in determining whether to issue a surveillance device warrant.

Of the 55 applications examined, only three addressed privacy in what this office assesses to be sufficient detail. It is the view of this office that the issuing officer would benefit from knowing:

- what surveillance device(s) will be used (s 14(5)(a)(ii))
- how and when (at what times) the surveillance device(s) will be used to collect information
- where the device will be used (with as much detail as possible)
- what sort of information (including audio, visual and/or location) about people is likely to be obtained from the device
- whose conversations and activities are likely to be recorded (including persons of interest and others).

The use of a surveillance device may well be highly intrusive in a person's private life. In other cases, the extent to which a person's privacy will be affected may be minimal in comparison. The issuing officer should be given an idea of what is likely to be seen or heard from use of the device.

The ACC has acknowledged the issue while noting that it is a matter for the issuing officer to balance privacy and other considerations. However, the ACC

also advised that the issue is addressed in some detail in its new Electronic Intelligence Compliance Training Program.

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 have proper regard to this issue as required by s 16(2)(c) of the Act.

Conditions prompt in warrants

Section 17(1)(b)(xi) of the Act states that a surveillance device warrant must specify any conditions subject to which premises may be entered, or a surveillance device may be used, under the warrant. Under the Act, the authority of a warrant is subject to any specified conditions.

It is generally the case that the ACC drafts and prepares the warrant for the issuing officer to sign. It was the view of this office that it would be best practice to include a prompt for the issuing officer to alert them to consider whether any conditions should be imposed.

Approximately half of the warrants inspected did not contain wording to prompt an issuing officer to impose conditions if they so chose. The ACC indicated that the issue is covered in the new Electronic Intelligence Compliance Training Program.

Recommendation

The Australian Crime Commission should ensure that all warrants contain a conditions paragraph, to assist the issuing officer in deciding if conditions should be imposed.

Other issues

Sections 20 and 21 of the Act require the chief executive 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 executive officer must take steps to ensure that use of the surveillance device is discontinued.

There was one instance of a substitute revocation instrument being signed when documentation could not be found for an earlier attempt to revoke a warrant. It is the view of this office that if the earlier attempt at revocation was not valid under the Act, the warrant expired naturally and therefore a substitute revocation need not have been issued.

Comment regarding the most recent inspection

After each inspection by this office, a draft report is prepared and provided to the inspected agency for comment before a final report is made. This process is procedurally fair to the agency reported on and ensures accuracy. It can also take some time, and this often means that an inspection in one six-month period is not reported on under s 61 of the Act until the subsequent six-month period. As advised earlier in the report, it was agreed between this office and the AGD that it would be necessary to finalise the report of an inspection before those results are included in this report.

Although it is not my intention to discuss the findings of the most recent inspection (September 2008), as the report of that inspection is not yet finalised, it is worth noting that the findings from that inspection are positive, and it is clear that certain initiatives of the ACC have had an impact upon their level of compliance. During the March 2008 inspection, this office was advised that an Electronic Intelligence Compliance Training Program had commenced, surveillance device administration had been centralised within the EPMC and that considerable effort had been applied to achieving excellence in compliance. The improvements from these changes were quite apparent during the September inspection.

AUSTRALIAN FEDERAL POLICE

Inspection results

The results of one inspection of the AFP's surveillance devices record was finalised in the reporting period. The inspection was carried out from 31 March 2008 to 4 April 2008 at the AFP's Telecommunications Interception Division. The inspection examined 70% of the AFP's eligible records (103 out of 147 records). A final report was provided to the AFP on 15 October 2008.

Based on the examination of the 103 records, the AFP was assessed as generally compliant with the provisions of the Act. Overall, the records examined were of a high standard. However, one recommendation was made concerning compliance with the Act and two recommendations were made to improve administration in relation to the Act.

A significant improvement was noted in the level of content provided in reports to the Minister under s 49 of the Act—a matter commented upon in previous reports.

A subsequent inspection was conducted in September 2008. The results of this inspection are yet to be finalised and are not included in this report.

Compliance issues

One recommendation was made relating to an issue of compliance.

Extraterritorial operation of warrants

The AFP sought a warrant for a surveillance device to track the movements of a vessel that was berthed in a foreign country's waters. The warrant was issued more than a week after the tracking device had been installed and activated on the vessel. Section 18 establishes the requirement for a surveillance device warrant to authorise the installation and use of a surveillance device on specified premises. Section 6 of the Act defines premises to include a vehicle and vehicle is further defined as including a vessel.

Section 42(1) of the Act states that when considering an application for an extraterritorial warrant, the issuing officer must not permit the warrant to authorise that surveillance unless they are satisfied that the surveillance has been agreed to by an appropriate consenting official of the foreign country.

Section 14 of the Act sets out the information required in an application; it has no provision that requires an application for an extraterritorial warrant to state

that the surveillance has been agreed to by the officials of the foreign country. However, this is information that the issuing officer must be aware of before issuing the warrant under s 42(1) of the Act. Therefore, as a matter of necessity, the application for an extraterritorial warrant and the warrant itself, should contain such information.

The Commonwealth Director of Public Prosecution (CDPP) Surveillance Devices Manual provides guidance to Commonwealth law enforcement agencies on the application for, and drafting of, warrants. The CDPP Manual includes a standard template for warrants, which can be customised as appropriate, depending on the circumstances of each warrant. The Manual states that if investigators intend using a surveillance device in a foreign country, the application should provide full details relating to the use of the device or devices and information relating to the approval by a appropriate foreign official. It also states that the warrant should record the extra-territorial nature of the authority. These requirements were not satisfied in this instance.

The particular warrant was extended five times, providing authority for the use of the device for a period of 18 months. Section 42(6) requires that where a surveillance device warrant authorises the use of a device in a foreign country, as soon as practicable after the commencement of surveillance under the authority of a warrant, written evidence must be provided to the Minister that the surveillance was agreed to by an appropriate consenting official of the foreign country. This did not occur. The AFP undertook to advise the Minister immediately following our inspection.

It should be noted that it is the policy of this office not to inspect the records relating to the use of surveillance devices where those devices are in use. Consideration will be given to amending that policy where the use of a surveillance device is extended beyond a six month period.

Recommendation

The Australian Federal Police should ensure it complies with s 42 of the Act by obtaining a warrant before installing a surveillance device in a foreign country, and by providing the Minister with written evidence that the surveillance has been agreed to by an appropriate official of the foreign country. In addition, where a surveillance device will be used extraterritorially, warrants and warrant applications should contain paragraphs referring to its extraterritorial operation and to the fact that an appropriate official of the foreign country has agreed to the use of the device.

Installation of device on premises without permission

Section 39 of the Act provides for the use of a tracking device once approved by an appropriate authorising officer. Such an authorisation does not permit installation or retrieval of a tracking device if the installation or retrieval of the device involves entry onto premises without permission or an interference with the interior of a vehicle without permission. In one case, a tracking device was installed on a vehicle while it was in the driveway of a residence. The installation occurred without permission from the occupier of the premises.

Section 53 register

Section 53 of the Act requires a register of all warrants and authorisations to be kept. In the first half of 2007 the AFP developed a new electronic database to maintain a register of warrants and authorisations.

The register is required 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:

- the name of the law enforcement officer primarily responsible for the execution of the warrant or to whom the authorisation was given
- details of the relevant offence or child recovery order for which the warrant or authorisation was issued
- the period the warrant is to be in force
- details of any variation or extension of the warrant.

The register was found to be substantially correct, although some minor errors were noted, most likely as result of the recent transfer of data from the old register.

Administrative issues

Two recommendations were made to improve administration in relation to the Act.

Destructions

This was only the second inspection in which the AFP had destroyed records relating to the use of a surveillance device. Section 46(1)(b) states that the chief officer of a law enforcement agency must cause to be destroyed every record or report comprising protected information as soon as practicable after the making of the record or report, if the chief officer is satisfied that no civil or criminal proceeding to which the material contained in the record or report relates has been, or is likely to be, commenced and that the material contained

in the record or report is not likely to be required. Section 46(1)(b) also requires the destruction of a record or report within a five year period of the making of the record or report.

In three of the files inspected, it was not clear from the information on file if the records and reports had in fact been destroyed. The AFP advised that they were due to be destroyed but this had not occurred at the time of the inspection.

There appears to be an issue of delay. In one case the time between approval of the destruction and the actual destruction was over nine months. Such a delay does not appear to meet the requirement that the destruction occur 'as soon as practicable'.

The AFP advised that the delay was due to a combination of administrative problems and the availability of and access to incinerators in the regional offices. It has been arranged that material from regional offices can be moved to Canberra for destruction.

Recommendation

The Australian Federal Police should establish policies and procedures to ensure that records and reports are destroyed as soon as practicable after the chief officer has approved the destruction. In addition, the AFP should ensure that all the recordkeeping relating to destructions is accurate and complete.

Installation of a device before a warrant is issued

Section 18 of the Act states that a surveillance device warrant authorises the installation and use of a surveillance device in or on a specified object or class of object. During the inspection it was noted that there was one instance of a listening device and a tracking device being installed in an object (a box from an overseas destination) seven hours before the warrant was issued.

The AFP has been advised that where it has control over a package, it may install a device before the warrant or authorisation is granted as long as it is not actually used before then. However, the AFP understands that there are risks to the admissibility of evidence obtained under such circumstances. Although in this case the information was not used as evidence, it is considered better practice for the AFP to wait until a warrant is issued before installing a device. The AFP has indicated that it shares this view.

Privacy

Section 16(2) of the Act sets out those matters that issuing officers 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'.

Although most warrant applications made reference to the effect the surveillance device would have on privacy, there was a general lack of detail, and 12 applications did not make any reference to privacy. This issue has been raised in several inspection reports to the AFP. While an improvement has been noted in the number of applications addressing privacy and the manner in which they do so, there remains scope for further improvement.

The AFP has acknowledged the importance of providing as much information as possible in relation to privacy to the issuing officer. Privacy continues to be a part of training, workshops and discussions.

Recommendation

The Australian Federal 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 use of a surveillance device, so that issuing officers can more readily address the requirements of s 16(2)(c) of the Act.

Prof. John McMillan
Commonwealth Ombudsman