Commonwealth OMBUDSMAN

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

INSPECTIONS FINALISED BETWEEN 1 JANUARY – 30 JUNE 2010

AUSTRALIAN CRIME COMMISSION
Records from 1 January 2009 to 30 June 2009

AUSTRALIAN FEDERAL POLICE
Records from 1 January 2009 to 30 June 2009

CORRUPTION AND CRIME COMMISSION (WA)
Records from 1 July 2008 to 30 June 2009

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

November 2010

ISSN 1833-9263

Date of publication: November 2010
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. It establishes procedures to obtain permission to use such devices in relation to criminal investigations and the recovery of children, and imposes requirements for the secure storage and destruction of records in connection with surveillance device operations.

Section 55(1) of the Act requires the Commonwealth Ombudsman to inspect the records of each law enforcement agency to determine the extent of compliance with the Act by the agency and its law enforcement officers.

Under s 6(1) of the Act, the term 'law enforcement agency' includes the Australian Crime Commission (ACC), the Australian Federal Police (AFP), the Australian Commission for Law Enforcement Integrity (ACLEI), police forces of each State and Territory, and specified State and Territory law enforcement agencies, such as the WA Corruption and Crime Commission (CCC).

The Ombudsman is also required under s 61 of the Act to report to the relevant Minister (the Attorney-General) at six-monthly intervals on the results of each inspection. Reports to the Minister alternately include the results of inspections that have been finalised in the periods January to June and July to December. Inspection results are considered finalised once the Ombudsman's report to the agency is completed (having provided the agency with an opportunity to comment). Typically then, there will be some delay between the date of inspection and the report to the Minister.

The following is a summary of the inspections to which this report relates.

Table 1: Inspections which were finalised between 1 January and 30 June 2010

Agency	Records covered by inspection	Date of inspection	Report to the agency completed
ACC	1 January to 30 June 2009	24 to 27 August 2009	29 April 2010
AFP	1 January to 30 June 2009	12 to 16 October 2009	9 April 2010
CCC	1 July 2008 to 30 June 2009	13 November 2009	2 March 2010

Detailed reports on the results of each inspection were provided to the relevant agency. This report summarises the results of these inspections, outlining

significant compliance and administrative issues. One recommendation has been made with respect to each of the three agencies reported on.

CONDUCT OF INSPECTIONS

All records held by an agency that relate to warrants and authorisations issued under the Act 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 were revoked during the inspection periods.

This office appreciates the continued cooperation of the agencies inspected and their constructive responses to address the issues identified. The importance agencies place on compliance with the Act and their efforts to implement the recommendations made by this office is recognised.

SUMMARY OF AGENCY COMPLIANCE

Australian Crime Commission

The ACC continues to improve practices relating to compliance. It is responsive to the recommendations made by the Ombudsman and has incorporated our input into policy and training.

The main issue we raised relates to the practice of combining applications for telecommunications intercepts and the use of surveillance devices. The two relevant Acts are: the *Surveillance Devices Act 2004* (the Act), and the *Telecommunications (Interception and Access) Act 1979* (TIA Act).The practice of making a combined application under both Acts is acceptable provided that the requirements of both are satisfied.

During the reporting period, we identified a number of areas where the requirements of the Act had not been satisfied under a dual application. The ACC accepted our findings and has reviewed procedures and training to address this issue.

Another issue we raised was the practice of obtaining new surveillance device warrants to retrieve devices which could have been retrieved under the authority of the original surveillance device warrant or under a retrieval warrant (if the original surveillance device warrant had expired). The ACC did not accept our finding and maintained that the additional surveillance device warrants were justified.

Both of these issues are discussed in greater detail under 'Australian Crime Commission – Issues arising from the inspection'.

Australian Federal Police

We noted a high level of compliance for the AFP during this reporting period.

The most significant issue we raised relates to the requirement that the original applicant or someone acting on behalf of the original applicant may only apply for an extension or variation for a warrant. In a number of instances this did not occur. The AFP accepts our view and is aware of the requirements of the Act. It disclosed this issue to the Ombudsman prior to the inspection and is addressing it with the relevant areas.

This issue is discussed in greater detail under 'Australian Federal Police – Issues arising from the inspection'.

Corruption and Crime Commission (WA)

This was the first inspection of the CCC and involved an examination of records relating to one warrant. Procedures were well documented and record keeping was of a high standard.

The warrant in question was extended twice. In its own report to the Minister (required under s 49 of the Act) the CCC must report details of such extensions. This did not occur and we consequently made a recommendation that future Ministerial reports contain this information. The CCC accepted the recommendation.

This issue is discussed in greater detail under 'Crime and Corruption Commission – Issue arising from the inspection'.

AUSTRALIAN CRIME COMMISSION

Inspection results

The inspection of Australian Crime Commission (ACC) surveillance device records was conducted at the ACC's Electronic Product Management Centre (EPMC) in Sydney from 24 to 27 August 2009. The inspection examined surveillance device warrants and authorisations (and associated records) that expired during the period 1 January to 30 June 2009. A report of this inspection was provided to the ACC on 29 April 2010.

Based on the examination of 53 warrants and authorisations, the ACC was assessed as compliant with the Act. One recommendation to improve compliance was made as a result of the inspection and a number of issues were noted where improvement is required.

ACC improvements

The ACC has implemented a training program directed at improving compliance in the use of special powers. The training is managed by the EPMC and is strongly supported by senior management. We are advised that the training program has recently been revised to incorporate recommendations made by the Ombudsman.

The ACC has amended its 'register of warrants, emergency authorisations and tracking device authorisations' (required under s 53 of the Act) to better distinguish between the date a warrant is extended and the date the extension takes effect. This is in response to an issue raised in the Ombudsman's previous report highlighting possible confusion over the expiry date of an extension.

Issues arising from inspection

Application for warrants under the Telecommunications (Interception and Access) Act 1979 and the Surveillance Devices Act 2004

The ACC generally uses a single application to apply for both an interception warrant and a surveillance device warrant where both powers are to be used in respect to the same investigation. We noted that the Surveillance Devices Manual issued by the Commonwealth Director of Public Prosecutions discusses dual applications, including standard forms for applications and affidavits that comply with the requirements of both Acts.

We accepted that it would often be more economical and practical to combine the applications for an investigation. However, dual applications must meet the requirements of both Acts. In some cases the applicant addressed only the requirements of the TIA Act.

'Serious offences' and 'relevant offences'

An interception warrant is issued in relation to a 'serious offence', whereas a surveillance device warrant is issued in relation to a 'relevant offence'.

'Serious offence' under s 5D of the TIA Act refers to a number of offences, including money laundering and serious drug offences, such as trafficking.

'Relevant offences' under s 6 of the Act includes an offence against the law of the Commonwealth (or a law of a State that has a federal aspect) that is punishable by a maximum term of three years or more, or for life.

In one particular dual application (for an interception warrant and a surveillance device warrant), that is, that the application addressed the requirement that the information likely to be obtained under an interception warrant would assist in the investigation of 'serious offences'. However, the application did not demonstrate reasonable grounds to suspect that 'relevant offences' had been, were being, were about to be, or were likely to be, committed, and that the use of a surveillance device was necessary to collect evidence for 'relevant offences' under s 14(1) of the Act.

In our opinion, although the particular offences appear to satisfy both criteria, the requirements under each Act should be addressed separately and explicitly.

Previous warrants sought or issued

Both Acts require the issuing officer to consider any previous applications that the agency has made in relation to the same telecommunication service or person (TIA Act), or the same alleged offence or recovery order (the Act). It is therefore incumbent upon the applicant to provide such detail where applicable.

Several of the applications we examined only referred to previously issued interception warrants, although it appeared that surveillance device warrants had also been issued in respect of the matter. Even where no surveillance device warrants were issued for the same alleged offence or recovery order, this should be made clear in the application.

Warrant extensions

An interception warrant cannot be extended, whereas a surveillance device warrant can be extended, with each extension lasting a further 90 days. In one case, the continued use of interception powers and surveillance devices was sought under a dual application. While a fresh warrant under the TIA Act may be required, extension provisions are available under the Act. They provide a simplified means of extension that also ensures the issuing officer is aware that surveillance upon a particular person, premises or object will extend beyond the usual three months.

Privacy

The extent to which the privacy of any person is likely to be affected is a consideration for the issuing officer under both Acts. In several dual applications privacy considerations were addressed for intercepting telecommunications, but not for the use of surveillance devices.

Recommendation 1: Australian Crime Commission

When using a dual application to apply for a warrant under the *Telecommunications (Interception and Access) Act 1979* and for a warrant under the *Surveillance Devices Act 2004,* the Australian Crime Commission should ensure that the application addresses the requirements under both Acts.

Warrants obtained for devices installed under previous warrants

Previous surveillance

A number of warrants were obtained in relation to devices already installed under earlier warrants. While this is permitted under the Act, two of the applications for the later warrants did not refer to the previous warrants. Section 16(2)(f) of the Act states that the issuing officer must have regard to any previous warrant sought in connection with the same alleged offence. Therefore, sufficient reference to previous warrant(s) should be made so as to provide the issuing officer with a full understanding of the circumstances.

Overlapping warrants

A surveillance device warrant was issued for a period of 90 days (the first warrant). This warrant authorised the use of listening, tracking, optical and data surveillance devices with respect to the conversations, activities or location of the target. Under s 18(2)(c) of the Act, this warrant permits the installation, use

and maintenance of a surveillance device on premises where the target is reasonably believed to be or likely to be. Section 18(3) of the Act authorises the retrieval of installed devices.

Under the first warrant, a number of surveillance devices were installed at different premises. Three separate warrants were later obtained with respect to premises the target was believed to attend. Two of these three warrants were executed and the devices that were installed under the first warrant were retrieved. Retrieval of the devices occurred under the authority of the subsequent warrants while the first warrant was still in force.

It would have been more appropriate to retrieve the devices under the authority of the first warrant. If there was any concern that the warrant would expire before the devices were retrieved, then the extension provisions under s 19(1) of the Act should have been used. Alternatively, a retrieval warrant could have been used.

The use of overlapping warrants has in the past led to instances of non-compliance with the Act due to confusion over which warrant conferred the authority for conducting surveillance activities and retrieval of devices. It is not the intention of this office to involve itself in operational decisions but to identify practices that may ultimately lead to devices being used unlawfully.

AUSTRALIAN FEDERAL POLICE

Inspection results

The inspection of Australian Federal Police (AFP) surveillance device records was conducted at the AFP's Telecommunications Interception Division (TID) in Canberra from 12 to 16 October 2009. The inspection examined a sample of surveillance device warrants and authorisations (and associated records) that expired during the period 1 January to 30 June 2009. A report of this inspection was provided to the AFP on 9 April 2010.

Based on the examination of 88 (out of a possible 165) warrants and authorisations, the AFP was assessed as compliant with the Act. One recommendation to improve compliance was made as a result of the inspection and a number of issues were noted where improvement is required.

Issues arising from inspection

Extension and variation of surveillance device warrants

Section 19 of the Act outlines the requirements for agencies when extending or varying a surveillance device warrant. Section 19(1) states that the law enforcement officer to whom a surveillance device warrant has been issued (or another person on his or her behalf) may apply for an extension.

Five of the applications to extend warrants were not made by the original applicant, or a person acting on behalf of the original applicant. The AFP is aware of the requirements of s 19(1) and disclosed this error during the inspection. The AFP accepted our recommendation and is addressing the issue.

Recommendation 1: Australian Federal Police

The AFP should ensure that applications to extend or vary a surveillance device warrant satisfy the requirements of section 19 of the *Surveillance Devices Act 2004* and are made by the original applicant for the warrant or by another person on his or her behalf.

Access to premises

Section 18 of the Act sets out the types of surveillance device warrants which may be issued and the activities permitted under each type of warrant. A surveillance device warrant may be issued in relation to premises, objects or

persons. Each type of warrant allows police to access certain premises to install the surveillance device.

A *premises* warrant allows access to:

- the premises on which the surveillance device is to be installed (which must be specified in the warrant)
- any adjoining premises or premises providing access to where the device will be installed (which must also be specified in the warrant).

An *object* warrant allows access to:

- any premises where the object, or an object of a class specified in the warrant, is reasonably believed to be or is likely to be
- any adjoining premises or premises providing access to where the device will be installed.

A *person* warrant allows access to:

- any premises where the particular person is reasonably believed to be or is likely to be
- any adjoining premises or premises providing access to where the device will be installed.

All records examined relating to 'premises' warrants showed that the premises entered by the AFP to install the surveillance device were permitted by the warrant. However, for 'object' and 'person' warrants it was not always possible to determine if this was the case. In relation to one 'object' warrant, it was unclear from the records whether the premises entered by the AFP were premises where the object was reasonably believed to be or likely to be. In relation to four 'person' warrants, it was unclear from the records whether the premises entered by the AFP were premises where the person was reasonably believed to be or likely to be.

As 'object' and 'person' warrants do not specify the premises to which entry is permitted, it would be appropriate for the AFP to keep records which demonstrate that any entry to premises under an 'object' or 'person' warrant is authorised by the warrant.

CORRUPTION AND CRIME COMMISSION (WA)

Inspection results

An inspection of WA Corruption and Crime Commission (CCC) surveillance device records was conducted at the CCC premises on 13 November 2009. The inspection examined surveillance device warrants and authorisations (and associated records) that expired during the period 1 July 2008 to 30 June 2009. A report of this inspection was provided to the CCC on 2 March 2010.

Based on an examination of records for one surveillance device warrant (and two associated extensions), the CCC is assessed as compliant with the Act. One recommendation to improve compliance was made as a result of the inspection and a number of issues were noted where improvement is required.

This was the first inspection of records held by the CCC in relation to its use of the provisions of the Act. The CCC presented as an organisation concerned about compliance and quality assurance measures, and had adopted an approach that encouraged the continuous improvement of its administrative and compliance practices.

The CCC provided particularly detailed records relating to the use of surveillance devices at the inspection. Use of devices is not always well documented by agencies and we commended the CCC for adopting such good practice in this area. We are consequently able to give a high level of assurance to the Attorney-General that the surveillance undertaken by the CCC is conducted lawfully.

Issue arising from inspection

Detailing the number of extensions and reasons for them

Section 49(2)(c) of the Act requires the CCC's report to the Minister on each warrant to state the number of extensions granted and the reasons for these extensions.

In relation to the surveillance device warrant inspected, the period during which the warrant was in force was extended twice. The report required by s 49 included the period during which the warrant was in force (which was clearly longer than 90 days), but not the number of extensions granted or the reasons for these extensions.

Recommendation 1: Corruption and Crime Commission

The Corruption and Crime Commission should ensure that its reports to the Minister under section 49 of the *Surveillance Devices Act 2004* contain details of the number of extensions (and variations) to surveillance device warrants or authorisations, and the reasons for these extensions (and variations).

Allan Asher
Commonwealth Ombudsman