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 2008 to 31 December 2008

AUSTRALIAN FEDERAL POLICE
1 January 2008 to 31 December 2008

NEW SOUTH WALES POLICE
1 July 2007 to 31 December 2008

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

March 2010

ISSN 1833-9263

Date of publication: March 2010
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.

Copies of this report are 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, 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 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, police forces of each State and Territory, and specified State and Territory law enforcement agencies.

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. Reports to the Minister alternately include the results of inspections that have been finalised in the periods January to June and July to December. Results are finalised once the Ombudsman's report to the agency is completed, so typically there will be some delay between the end of inspections and this report being made available.

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

Agency	Records covered by inspection	Date of inspection	Report to the agency completed
ACC	1 January 2008 to 30 June 2008	18 to 21 August 2008	Combined report: 20 August 2009
	1 July 2008 to 31 December 2008	16 to 19 February 2009	
AFP	1 January 2008 to 30 June 2008	15 to 19 September 2008	18 September 2009
	1 July 2008 to 31 December 2008	23 to 27 March 2009	18 September 2009
NSW Police	1 July 2007 to 31 December 2008	7 to 8 April 2009	5 November 2009

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.

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 been revoked during the inspection periods.

This office appreciates the continued cooperation of those 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 should be recognised.

OVERVIEW OF AGENCY COMPLIANCE

Our inspection team has noted continued improvement in agency compliance with the requirements of the Act. The majority of issues were relatively minor and generally able to be remedied through training and better recordkeeping practices. The agencies have willingly accepted our recommendations and have continued to improve administration of their surveillance device regimes.

The main issue arising from the inspections to which this report relates was a tendency by agencies to obtain successive surveillance device warrants for a single matter, rather than using the extension provisions in the Act. There was also a tendency to obtain multiple warrants (or tracking device authorisations) with respect to a target, where in our opinion a single person warrant would have sufficed. For example, separate warrants and tracking device authorisations might be obtained with respect to a person, the person's premises and objects belonging to the person, with the timeframe of subsequent warrants or authorisations overlapping.

It appears that the intention is to take a conservative approach and ensure that there is a warrant in place to cover all eventualities. While this practice is not prohibited by the Act, the use of multiple warrants and authorisations is, in many cases, unnecessary and can raise questions such as which warrants were executed and which were not, dates of expiry and the like. As such, there is a greater likelihood that a device will be inadvertently used without proper authority. The Act provides for varying and extending warrants to meet the exigencies that would arise in most circumstances, and these provisions should be used as intended. This issue is discussed in further detail in this report.

AUSTRALIAN CRIME COMMISSION

Inspection results

Inspections of ACC surveillance device records were conducted at the ACC's Electronic Product Management Centre (EPMC) in Sydney from 18 to 21 August 2008 and 16 to 19 February 2009. The first inspection examined surveillance device warrants and authorisations (and associated records) that expired during the period 1 January to 30 June 2008. The second inspection examined surveillance device warrants and authorisations (and associated records) that expired during the period 1 July to 31 December 2008. The combined report to the ACC on the results of the inspections was finalised on 20 August 2009.

Based on the examination of 106 warrants and authorisations (57 in the first inspection and 49 in the second inspection), the ACC was assessed as compliant with the Act. Four recommendations were made, comprising one compliance and three administrative issues.

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

ACC improvements

It was evident that the centralisation of surveillance device record administration within the EPMC and the implementation of training programs for the users of surveillance devices under the ACC's 'Excellence in Compliance Strategy' has significantly improved ACC compliance with the Act and records administration. Two of the more notable areas of improvement were:

- A substantial increase in compliance by the ACC in relation to the content, accuracy and timeliness of s 49 reports to the Minister. In previous inspections we had noted regular errors and omissions in these reports. Apart from a small number of exceptions, these errors and omissions were absent from recent records.
- A more proactive approach to revocation of warrants under ss 20 and 21. No warrant was permitted to remain in force once use of the surveillance device under the warrant had ceased. Although there is no strict requirement under the Act to revoke a warrant, even if the authority under the warrant will not be used or has ceased to be used, revocation of the warrant, in lieu of simply leaving the authority open until expiry of the warrant, is considered good practice.

Issues arising from inspection

The following issues were raised with the ACC as a result of our inspections, and where appropriate a recommendation made.

Person responsible for warrant execution

When a law enforcement officer ceases to be primarily responsible for executing a warrant or authorisation, s 6(3) of the Act allows the chief officer of a law enforcement agency to nominate another person by a written instrument. Section 6(3)(b) states that the change has 'effect from the execution of the instrument or such later time as is specified in the instrument'.

In one case, the person originally responsible for executing a warrant ceased to be a member of the ACC. The Chief Executive Officer of the ACC signed an instrument on 1 July 2008 purporting to retrospectively change the person primarily responsible for executing the warrant, effective from 27 June 2008. A device was installed under this warrant on 1 July 2008, and it was not possible to tell from the records whether this occurred at a time before or after the Chief Executive Officer signed the instrument. Given the wording of s 6(3)(b), it appears that the law enforcement officer primarily responsible for the execution of a warrant cannot be changed retrospectively.

Recommendation

The Australian Crime Commission should ensure that, where it becomes necessary to change the person primarily responsible for executing a warrant, this is done in a timely fashion.

Privacy

Section 16(2) of the Act sets out those matters that an eligible Judge or a nominated AAT member must have regard to when issuing 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)). Many applications inspected did not provide facts relating to a person's privacy to the issuing officer.

The considerable invasion of privacy resulting from the use of surveillance devices in or on private premises gives rise to the general prohibition under the Act. As such, it would seem important for law enforcement agencies to address this issue when making applications for warrants in order to aid the considerations that must be undertaken by issuing officers.

In response to the following recommendation, the ACC advised that it has adopted strategies to address this issue, including reviewing internal guidelines, emphasising the issue in training sessions and focusing on privacy requirements during internal audits.

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.

Applications for warrants—same alleged offence

Section 16(2)(f) of the Act requires an issuing officer to have regard to 'any previous warrant sought or issued under this Division in connection with the same alleged offence or the same recovery order'.

In some cases, applications for named person warrants only referred to previous applications in relation to the same person, and did not mention that warrants had been sought and granted for other people involved in the same matter and in relation to the same offences. In one case, a warrant was sought for a particular location and no mention was made that a device had already been installed at the same premises under a related warrant. This does not aid the issuing officer's consideration of related warrants and may not present a complete picture of the circumstances.

Recommendation

The Australian Crime Commission should ensure that all warrant applications include information on other warrants sought in relation to the same alleged offence(s), so that issuing officers can have proper regard to this issue as required by s 16(2)(f) of the Act.

Applications for warrants—devices already installed

Section 19 of the Act permits a law enforcement officer to apply, at any time before the expiry of the warrant, for an extension of the warrant for up to 90 days. The application is to be made to an eligible Judge or to a nominated AAT member, and if the application is granted the authorising officer endorses the new expiry date on the original warrant.

The provisions of s 19 were not always used by the ACC to extend the use of a surveillance device beyond the 90 day limit of the original warrant. On a

number of occasions a new warrant was sought for the use of a surveillance device already in place. While there is nothing in the Act that prohibits obtaining a new warrant in such circumstances, the concern is that the application for the new warrant was generally accompanied by the same affidavit provided with the application for the first warrant, which did not mention that the device was already in place.

The process under s 19 is to ensure that issuing officers are aware that a device has been in place for a period approaching 90 days and that they will be extending the use of the device for a further period of up to 90 days. The authorising officer is then in a position to turn their mind to the cumulative effect the extension might have on a person's privacy.

Recommendation

The Australian Crime Commission should ensure that, where a device has already been installed and it is proposed to continue to use that device under a new warrant/authorisation, the relevant application includes information on the installed device(s).

Information shared with State police forces

Section 49(2)(b)(xi) of the Act requires that the Minister be advised of 'details of the communication of evidence or information obtained by the use of the device to persons other than officers of the agency'. Section 52(1)(f) requires the chief officer of a law enforcement agency to keep details of such communications.

The ACC undertook a number of joint operations with State police forces. Two of the reports to the Minister under s 49 advised that information had been communicated to officers of the NSW Police, but no details were provided, nor were details of the communications recorded pursuant to s 52(1)(f).

The ACC later advised our office that the reports to the Minister were erroneous, and that the officers in question were actually seconded State police officers who were deemed to be officers of the ACC. Therefore, the requirements in ss 49(2)(b)(xi) and 52(1)(f) did not apply. The ACC indicated that it would provide revised reports to the Minister.

Although no formal recommendation was made in respect of this matter, the prevalence of joint taskforces, the possible sensitive information involved and the potential for seconding arrangements to facilitate communication of information between the ACC and State police forces without attracting the obligations under s 52(1)(f) of the Act, warrant consideration by the ACC of

information sharing arrangements that satisfy both the requirement and intent of this section of the Act.

Destructions

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 the record within a five year period.

The ACC destroyed two files within the inspection periods. The records were destroyed some four months after the Chief Executive Officer of the ACC had certified that they were no longer required. Whilst the destruction occurred within five years after making the records, as s 46(b)(i) requires destruction to occur as soon as possible, this office advised the ACC that destructions should occur in a more timely manner.

AUSTRALIAN FEDERAL POLICE

Inspection results

Inspections of AFP surveillance device records were conducted at the AFP's Telecommunications Interception Division (TID) in Canberra from 15 to 19 September 2008 and 23 to 27 March 2009. The first inspection examined a sample of surveillance device warrants and authorisations (and associated records) that expired during the period 1 January to 30 June 2008. The second inspection examined a sample of surveillance device warrants and authorisations (and associated records) that expired during the period 1 July to 31 December 2008. The reports of these inspections were both finalised and provided to the AFP on 18 September 2009.

Based on the examination of 80 (out of a possible 159) warrants and authorisations during the first inspection, and an examination of 84 (out of a possible 156) warrants and authorisations during the second inspection, the AFP is considered generally compliant with the requirements of the Act.

Three recommendations to improve compliance were made as a result of the first inspection and one recommendation was made following the second inspection.

AFP improvements

The AFP provided an additional quality assurance officer to assist TID with general recordkeeping. The AFP also instituted various measures to improve training of staff involved with surveillance processes. It was apparent in the inspections that the measures taken by the AFP have had a positive effect on the quality of recordkeeping required by the Act. In particular:

- Section 45 of the Act creates two offences relating to the use, recording, communication or publication of protected information, and sets out the circumstances that provide exemption from these offences. These circumstances are framed quite broadly. There is no requirement for 'approval' to be obtained before taking an action that would fall within one of the exemptions. Although there is no requirement, the AFP has adopted an internal practice of using 'certificates' signed by the Commissioner or a senior officer in instances where the dissemination of protected information would incur particular sensitivities. This practice, if used consistently, provides the AFP with an important accountability mechanism and helps to ensure that the dissemination of sensitive information is well managed.

- There was a significant improvement in the timeliness and recordkeeping related to destructions of records obtained by use of surveillance devices. The AFP advised that the process for destruction of material kept in regional offices has been centralised to further improve timeliness.

Issues arising from inspection

The following issues were raised with the AFP as a result of our inspections, and where appropriate a recommendation was made.

Installation, use and retrieval of tracking device

In one case examined, a warrant was obtained for a listening device for a known person (the person warrant). The person warrant was in force for a period of 90 days. Seven days after the warrant was issued, another officer applied for, and was granted, a tracking device authorisation for a car used by the person who was the subject of the person warrant. This authorisation (given separately under s 39 to the person warrant) was for a period of 30 days. Although a person warrant permits access to any premises or vehicles belonging to that person for the purpose of installing a device, the type of device or devices must be authorised in the warrant. The person warrant did not authorise the use of tracking devices.

It appears from the records that a device that comprised both a listening device and a tracking device was installed in or on a car belonging to the person in respect to whom the person warrant was issued. The device was installed while the car was parked on the premises of that person.

Section 39(8) states that permission to use, install or retrieve a tracking device must not be given if the installation of the device, or its retrieval, involves entry onto premises or interference with the interior of a vehicle without permission. Therefore, the installation of the tracking device was contrary to s 39(8). The installation of the tracking device was also not authorised by the person warrant.

Further, the combined device was retrieved seven days after the expiry of the tracking device authorisation. Although the retrieval occurred within the period of the person warrant, this warrant did not provide authority for dealing with a tracking device. The situation also suggests that product from the tracking device could have been obtained after the expiry of the authorisation.

Recommendation

The Australian Federal Police should ensure that the use of tracking devices under an authorisation does not involve entry onto premises or interference with the interior of a vehicle contrary to s 39(8) of the Act. It is further recommended that where a warrant is in place and an additional device is to be used in respect of the person or premises subject to the warrant, that a variation to the warrant be sought rather than a new warrant (or tracking device authorisation), particularly where a composite device is to be used.

Applications for warrants—devices already installed

The same issue was raised with the ACC and is discussed earlier in the report in more detail.

Section 19 of the Act permits a law enforcement officer to apply, at any time before the expiry of the warrant, for an extension of the warrant for up to 90 days. The AFP did not always use this provision and more often than not, a new warrant was sought to authorise the use of a surveillance device already in place. The application for the new warrant was generally accompanied by the same affidavit provided with the application for the first warrant, which did not mention that the device was already in place.

The process under s 19 ensures that authorising officers are aware that a device has been in place for a period approaching 90 days and that they will be extending the use of the device for a further period of up to 90 days. The authorising officer is therefore in a position to turn their mind to the cumulative effect the extension might have on a person's privacy.

Recommendation

The Australian Federal Police should ensure that the process set out in s 19 of the Act for the extension of a surveillance device warrant is utilised when extending the use of a surveillance device.

Applications for extension of surveillance device warrant

Section 19(1) of the Act permits a law enforcement officer to whom a surveillance device warrant has been issued, or another person acting on his or her behalf, to apply for an extension to a surveillance device warrant.

At both inspections, and in a number of applications for extension of a warrant, the applicant was not the officer to whom the original warrant was issued. Nor

did the applicant state that they were acting on behalf of the officer to whom the warrant was originally issued.

Recommendation

The Australian Federal Police should ensure that applications for extension to warrants comply with s 19(1) of the Act, in that the application for an extension should be made by the officer to whom the original warrant was issued or a person acting on his or her behalf.

Surveillance device terminology

Section 17(1)(b)(v) of the Act requires that the authorised surveillance device appears on a warrant. A surveillance device is defined in the Act to mean one of several types, or a combination of the defined types or a device of a kind prescribed by the regulations.

It was noticed that some warrants had specified the device to be used to be an 'opening device', which is neither defined in the Act nor set out in a regulation. Therefore, it is not a surveillance device under the Act. Although an 'opening device' is the name given to a particular type of tracking device, it is not recognised by the Act and may bring into question the validity of the warrant.

Recommendation

The Australian Federal Police should ensure that warrants authorise surveillance devices known to the Act or, alternatively, take steps to have new types of devices prescribed in an appropriate regulation.

Use of overlapping warrants

In one case examined, difficulties arose when there was a change to the registration number of a car which had been specified as 'premises' for the purposes of a surveillance device warrant.

A warrant had been issued for listening devices, tracking devices and optical surveillance devices in relation to a car with a particular registration number (the premises warrant). Concurrently, another warrant was issued for listening devices, data surveillance devices, tracking devices and optical surveillance devices in relation to a particular person for surveillance separate to the car (the person warrant). It appears the person owned or used the car that was the subject of the premises warrant, although the person warrant had been obtained for surveillance purposes other than those relating to the car.

A device was installed in the car under the premises warrant, while the person warrant remained unused. The registration number of the car changed, and it appears that there was some concern that the devices could not be retrieved under the premises warrant which identified the car by its registration number. The decision was taken to retrieve the device under the person warrant.

The authority of the person warrant permitted the retrieval of the device. However, it would have been preferable for the premises warrant to be varied (and extend if necessary) or seek a separate retrieval warrant in order to retrieve the device, rather than use the person warrant for a different purpose than that outlined in the application for that warrant.

Recordkeeping involving overlapping warrants

The process of applying for the issue of overlapping warrants to authorise devices already in place can cause a number of difficulties. One example is the reports under s 49 of the Act, which require the AFP to inform the Minister on certain matters relating to the use of surveillance devices under warrants and authorisations.

In one case, a warrant was sought to cover the use of a tracking device already installed on a vehicle under a previously issued warrant. The use and communication log for the second warrant indicated that information was obtained from the device during the term of the warrant. However, the report to the Minister under s 49 of the Act stated that the warrant was not executed. It also stated that that the device was covered by a third warrant, which we understood to be a person warrant also authorising the use of a tracking device.

When there was a series of overlapping warrants authorising the use of the same devices, the s 49 reports to the Minister generally gave a satisfactory overall explanation of the relationship of the warrants being reported on. However, it was also clear that there was uncertainty regarding the reporting of installation, use, communication and retrieval of information when such overlapping warrants were used. The better practice would be to avoid overlapping warrants whenever possible and make greater use of extension and variation provisions within the Act.

It was also noted that the affidavit for the second and third warrants included the affidavit for the first warrant as an annexure. The issuing authority might reasonably infer that the device was already in place. However, it would be preferable in these circumstances that this fact be specifically put before the issuing authority.

Privacy

Issuing officers must have regard to those matters sets out in s 16(2) of the Act 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)).

As discussed above for the ACC, it is the view of this office that matters concerning the privacy of individuals are central to the legislation, given the highly invasive nature of surveillance devices. Any facts relevant to the extent to which a person's privacy will be affected by issue of a surveillance device warrant should be set out in the supporting affidavit for consideration by the issuing officer.

However, it is also noted that considerable improvement has been made by the AFP since the previous inspections in respect to this issue, and therefore make no recommendation.

Destructions

The AFP had approved destruction of product in relation to 55 warrants in accordance with the requirements of the Act during the two inspection periods. Confirmation was also found on each file that the relevant product had been destroyed.

However, one file held a transcript of a conversation obtained by a surveillance device that was identified as having been destroyed. It was also apparent that products from several other warrants had been recorded on a laptop computer. It was unclear if, or when, the products had been removed from the computer. We suggested to the AFP that it more thoroughly document destruction processes in unusual circumstances.

NEW SOUTH WALES POLICE

Inspection results

An inspection of NSW Police surveillance device records was conducted at the office of the NSW Police Anti-Terrorism Group in Sydney on 7 and 8 April 2009. The inspections examined surveillance device warrants and authorisations (and associated records) that expired during the period from 1 July 2007 to 31 December 2008. A final report was provided to the NSW Police on 5 November 2009.

Based on an assessment of six warrants and associated records, NSW Police is assessed as compliant with the requirements of the Act. Overall, the records examined were of a high standard. Two recommendations were made.

NSW Police improvements

Significant improvement was noted in NSW Police compliance and general standards of recordkeeping in comparison with the previous inspection in November 2007. It was clear that the NSW Police had acted quickly and effectively in response to our earlier recommendations. The more notable improvements were:

- A substantial improvement in relation to the timeliness of reports provided to the Minister under s 49 of the Act. This office has adopted an interpretation that a three month period from the time the warrant ceased or was revoked would generally satisfy the requirement 'as soon as practicable'. All six of the reports inspected had been provided to the Minister within three months.
- In the previous inspection, nine of the 33 warrants did not detail the legislative provision under which the relevant offences were created. Instead, the nature of the offences was simply described on the warrants. No such problem was identified during this inspection.

Issues arising from inspection

The following issues were raised with the NSW Police as a result of our inspection, and where appropriate a recommendation made.

Communication with the AFP

Under s 52(1)(f) of the Act, the chief officer of a law enforcement agency must ensure that details are kept of each 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.

NSW Police officers and AFP officers worked together in the Joint Counter Terrorism Team. While this presents practical difficulties, as communication of information between the officers of this team is a necessary and regular event, s 52(1)(f) nonetheless applies. There was little documentation of communications between the NSW Police and the AFP despite actions taken by both agencies in response to information obtained by the NSW Police through the use of surveillance devices.

Recommendation

While the practical difficulties of logging communications with the AFP are noted, the NSW Police is currently in breach of s 52 of the *Surveillance Devices Act 2004* and should consider ways of addressing this non-compliance.

As noted above, the NSW Police had not logged its communications with the AFP in relation to the Joint Counter Terrorism Team. While the practical difficulties are acknowledged, the problem also affects the NSW Police's ability to comply with s 49(2)(b)(xi), namely the requirement to report to the Minister all communications of information. Consequently, many of the reports to the Minister under s 49 did not comply with this provision.

Privacy

There is still room for improvement regarding the amount of information provided by warrant applicants to address the issue of privacy under s 16(2)(c) of the Act. In general, the affidavits presented very little information relating to this issue.

As all six warrant applications related to one investigation, the understanding by investigators of those people (including non-targets) affected by the use of the device(s) would have increased over time. This should provide opportunity for each subsequent warrant application to use the increased understanding to assist the issuing officer to have regard to the likely effects on privacy. However, this did not occur. While the supporting affidavits were quite detailed, they did not focus on information that might assist the issuing officer to have regard to s 16(2)(c).

While this is only one criterion to be considered by the issuing officer, it is an important one given the intrusive nature of surveillance devices and that these

six warrants resulted in a situation where some people were under surveillance for a considerable period of time.

Recommendation

The NSW Police should ensure that warrant applications contain information allowing issuing officers to have proper regard to s 16(2)(c) of the *Surveillance Devices Act 2004*.

Use of assumed identities

Section 49 of the Act requires a report to be provided to the Minister, which necessarily includes the names of people undertaking certain activities. Where a person was an undercover operative, the NSW Police reported these people by use of an assumed identity in lieu of the person's actual name.

Although the Act requires a person's name to be identified in the report, there are significant security and safety issues that preclude strict compliance. We have discussed the matter with NSW Police and have agreed that the inclusion of undercover operative code numbers would satisfy the intent of the legislation, as they can be used to identify those officers involved in the use of a surveillance device.

Ron Brent
Acting Commonwealth Ombudsman