Commonwealth OMBUDSMAN

Report to the Commonwealth 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 2014

AUSTRALIAN COMMISSION FOR LAW ENFORCEMENT INTEGRITY
Records from 1 January to 30 June 2013

AUSTRALIAN CRIME COMMISSION
Records from 1 January to 30 June 2013

AUSTRALIAN FEDERAL POLICE
Records from 1 January to 30 June 2013

CRIME AND MISCONDUCT COMMISSION
Records from 1 July 2012 to 30 June 2013

NEW SOUTH WALES POLICE FORCE
Records from 1 September 2012 to 30 June 2013

VICTORIA POLICE
Records from 1 July 2012 to 30 June 2013

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

September 2014

Commonwealth OMBUDSMAN

Report to the Commonwealth 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 2014

AUSTRALIAN COMMISSION FOR LAW ENFORCEMENT INTEGRITY
Records from 1 January to 30 June 2013

AUSTRALIAN CRIME COMMISSION
Records from 1 January to 30 June 2013

AUSTRALIAN FEDERAL POLICE
Records from 1 January to 30 June 2013

CRIME AND MISCONDUCT COMMISSION
Records from 1 July 2012 to 30 June 2013

NEW SOUTH WALES POLICE FORCE
Records from 1 September 2012 to 30 June 2013

VICTORIA POLICE
Records from 1 July 2012 to 30 June 2013

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

September 2014

ISSN 1833-9263

Ownership of intellectual property rights in this publication

Creative Commons Licence

Use of the Coat of Arms

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

Copies of this report are available online from the Commonwealth Ombudsman website 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.[1] The Act also establishes procedures for law enforcement agencies 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 the use of surveillance devices.

Broadly speaking, the Act allows certain surveillance activities to be conducted under either a warrant (issued by an eligible Judge or nominated Administrative Appeals Tribunal member) or an internally issued authorisation. For example, use of surveillance devices requiring entry on to premises can only be done under a warrant, whereas use of surveillance devices which does not involve entry on to premises can be done without a warrant, but in some cases requires an internally issued authorisation.

Section 55(1) of the Act requires the Commonwealth Ombudsman (Ombudsman) to inspect the records of each law enforcement agency to determine the extent of their compliance with the Act. Under s 6(1) of the Act, the term 'law enforcement agency' includes the Australian Commission for Law Enforcement Integrity (ACLEI), the Australian Crime Commission (ACC), the Australian Federal Police (AFP), police forces of each state and territory such as the New South Wales (NSW) Police Force and the Victoria Police, and other specified state and territory law enforcement agencies such as the former Crime and Misconduct Commission (CMC).[2]

The Ombudsman is also required under s 61 of the Act to report to the relevant Minister (the Commonwealth Attorney-General) at six-monthly intervals on the results of each inspection. Reports to the Attorney-General 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 internal report to the agency is completed (having provided the agency with an opportunity to comment on the findings), so typically there will be some delay between the date of inspection and the report to the Attorney-General.

[1] Under the Act, a 'surveillance device' means a data surveillance device, a listening device, an optical surveillance device or a tracking device (or a device that is a combination of any two or more of these devices).

[2] The Crime and Corruption Commission replaced the CMC on 1 July 2014. As the inspection findings discussed in this report relate to the records of the former CMC, this report will refer to assessments made of the CMC.

The following table is a summary of the inspections covered by this report.

Table 1 – Inspections finalised between 1 January and 30 June 2014

				Finalised
Agency	**Inspection period**	**Dates of inspection**	**Number of records inspected**	**Report to the agency completed**
ACLEI	1 January to 30 June 2013	6 November 2013	5 / 5 warrants	7 April 2014
ACC	1 January to 30 June 2013	23-25 September 2013	78 / 78 warrants 5 / 5 TDA[3]s	26 February 2014
AFP	1 January to 30 June 2013	9-13 September 2013	105 / 313 warrants 10 / 22 TDAs	26 February 2014
CMC	1 July 2012 to 30 June 2013	29 August 2013	2 / 2 warrants	11 March 2014
NSW Police Force	1 September 2012 to 30 June 2013	26 September 2013	3 / 3 records relating to the retention of protected information	14 January 2014
Victoria Police	1 July 2012 to 30 June 2013	2 September 2013	2 / 2 warrants	14 January 2014

Detailed internal reports on the results of each inspection were provided to each agency. This report summarises the results of these inspections. We have not included sensitive information in this report.

[3] TDA means a 'tracking device authorisation'.

INSPECTION OBJECTIVE AND SCOPE

The objective of the inspection is to determine the extent of compliance with the Act by agencies and their law enforcement officers. The following criteria were applied to assess compliance:

1. **Were applications for warrants and authorisations properly made?**
   We determine this by assessing written records (applications and affidavits) against the legislative requirements.

2. **Were authorisations properly issued?**
   We determine this by assessing written records against the legislative requirements.

3. **Were surveillance devices used lawfully?**
   We determine this by comparing the details of what was permitted by the warrant or authorisation (i.e. the types of devices, the locations they may be used, the timeframes in which they must be used) with the surveillance conducted, as reported by the technical surveillance units.

4. **Were revocations of warrants properly made?**
   We determine this by assessing written records (instruments of revocation and warrants) against the legislative requirements.

5. **Were records properly kept by the agency?**
   We determine this by assessing written records, including the register of warrants and authorisations, against the legislative requirements.

6. **Were reports properly made by the agency?**
   We assess compliance with the requirements of ss 49 and 51(j), relating to reporting to the Attorney-General. We also assess the accuracy of these reports by reviewing the original records on which the reports are based.

7. **Was protected information properly dealt with by the agency?**
   We determine this by assessing written records (log sheets of use and communication of protected information, the register of warrants and authorisations and records relating to the destruction of protected information) against the legislative requirements.

All records held by an agency relating 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 inspections to those warrants and authorisations that had expired or were revoked during the relevant inspection period.

SUMMARY OF INSPECTION RESULTS

This report provides each agency's performance against the inspection criteria and discusses exceptions to compliance (including where we were unable to determine compliance) for each agency.

No recommendations were made as a result of these inspections, however, we made some suggestions as to how agencies can better comply with the relevant provisions of the Act. All six agencies displayed a positive attitude towards compliance and where applicable, were responsive to addressing the issues identified as a result of our inspections.

However, we identified an issue that we have previously reported on. This issue is about agencies providing our office with sufficient records to demonstrate that, when a warrant is issued in respect of a person, surveillance devices are only used on premises where that person is reasonably believed to be.

Requirements relating to 'person warrants'

Section 18(1)(c) states that a surveillance device warrant may authorise the use of a surveillance device in respect of the conversations, activities or location of a specified person or a person whose identity is unknown. A warrant of this type is colloquially known as a 'person warrant'. Section 18(2)(c)(i) states that a 'person warrant' authorises the installation, use and maintenance of devices on premises where the person is reasonably believed to be or likely to be. To allow operational flexibility, there is no requirement in the Act for a 'person warrant' to detail such premises.

However, this does not provide agencies with authority to install surveillance devices under a 'person warrant' on any premises. The premises, as s 18(2)(c)(i) requires, must be where the person is reasonably believed to be or likely to be. Therefore, where surveillance devices have been installed on premises under a 'person warrant', we would expect to see information relating to the use of these devices that connect the premises to the person named on the warrant.

If no, or insufficient, information is provided to make this connection, we are unable to verify compliance with s 18(2)(c)(i). This was the case for ACLEI and the AFP, as discussed under each agency's inspection results in the body of this report. We note that this is the first time this issue has been identified for ACLEI.

AUSTRALIAN COMMISSION FOR LAW ENFORCEMENT INTEGRITY

Inspection results

Criteria	Assessment
1. Were applications for warrants and authorisations properly made?	Compliant.
2. Were authorisations properly issued?	N/A
3. Were surveillance devices used lawfully?	Nothing to indicate otherwise except in one instance where we were unable to determine compliance.
4. Were revocations of warrants properly made?	N/A
5. Were records properly kept by the agency?	Compliant.
6. Were reports properly made by the agency?	Compliant.
7. Was protected information properly dealt with by the agency?	Nothing to indicate otherwise.

No recommendations were made as a result of the inspection carried out in November 2013. However, we were unable to determine compliance in one instance (discussed below). We also made one best practice suggestion to ACLEI regarding keeping contemporaneous records about surveillance activities, to better demonstrate compliance with criterion 3.

Exception noted under criterion 3

Access to records to confirm lawful access to premises under 'person warrants'

For one person warrant, there were no records on file to demonstrate that the surveillance devices were used on premises that the person was reasonably believed to be or likely to be. As a consequence we were unable to verify compliance with s 18(2)(c)(i) for this warrant (see page 4 for the Act's requirements relating to person warrants).

ACLEI has advised that, in response to this issue, it will update its procedures to strengthen its processes.

Progress made since previous report

There were no issues identified in our last report to the Attorney-General which required follow-up.

AUSTRALIAN CRIME COMMISSION

Inspection results

Criteria	Assessment
1. Were applications for warrants and authorisations properly made?	Compliant with one minor administrative issue noted.
2. Were authorisations properly issued?	Compliant with one minor administrative issue noted.
3. Were surveillance devices used lawfully?	Nothing to indicate otherwise.
4. Were revocations of warrants properly made?	Compliant.
5. Were records properly kept by the agency?	Compliant.
6. Were reports properly made by the agency?	Compliant with three administrative issues noted.
7. Was protected information properly dealt with by the agency?	Nothing to indicate otherwise, with one exception.

No recommendations were made as a result of the inspection carried out in September 2013. A small number of administrative issues were noted and we noted one instance where the ACC may not have complied with the Act (discussed below).

Exception noted under criterion 7

Destroying protected information

Section 46(1)(b)(i) of the Act requires that any record containing protected information be destroyed as soon as practicable after receiving the chief officer's approval to do so. The ACC advised that protected information obtained under one warrant was destroyed following the chief officer's approval to do so. However, the ACC self-disclosed that, at a later date, the "destroyed" protected information was retrieved from its systems and certified to be retained.

As the ACC did not complete the destruction of protected information obtained under this warrant to the extent where it was irretrievable, it may not have complied with s 46(1)(b)(i) in this instance.

Recognising this, the ACC self-disclosed this issue to the Ombudsman, and the ACC is to be commended for its transparency with our office. However, this issue has highlighted a need for there to be a common understanding across agencies regarding what constitutes the destruction of protected information under the Act.

Progress made since previous report

There were no issues identified in our last report to the Attorney-General which required follow-up.

AUSTRALIAN FEDERAL POLICE

Inspection results

Criteria	Assessment
1. Were applications for warrants and authorisations properly made?	Compliant with one exception and one administrative issue noted.
2. Were authorisations properly issued?	Compliant with one exception.
3. Were surveillance devices used lawfully?	Nothing to indicate otherwise with one exception. Unable to determine compliance in six instances.
4. Were revocations of warrants properly made?	Compliant with two administrative issues noted.
5. Were records properly kept by the agency?	Compliant.
6. Were reports properly made by the agency?	Compliant with five administrative issues noted.
7. Was protected information properly dealt with by the agency?	Nothing to indicate otherwise.

Although no recommendations were made as a result of the September 2013 inspection, we noted three instances of non-compliance and six instances where we were unable to determine compliance (all these instances are discussed below). A number of suggestions were also made regarding how the AFP could better comply with relevant provisions under the Act.

In addition, prior to the inspection, the AFP advised that 241 warrants and authorisations had ceased during the inspection period. We based our sample size on this figure and we inspected the records relating to 115 warrants and authorisations (a 34% sample). However, during the inspection we identified an anomaly between the information the AFP provided prior to, and during, the inspection. Following the inspection, the AFP advised that its initial advice was incorrect and that 335 warrants and authorisations (not 241) had ceased during the inspection period. The AFP has advised of measures it will take to ensure the accuracy of its statistical information it provides at future inspections.

As a consequence we can only provide confidence in the accuracy of our findings relating to the initial sample, as we were unaware of the existence of the additional records prior to, and at the time of the inspection. Furthermore, the risk analysis undertaken to determine our sample size for this inspection cannot be relied on as no consideration was given to the risks associated with the additional records that had ceased during the inspection period.

Although invited to, we were unable to re-attend the AFP to inspect the additional records due to our office's requirement to undertake multiple other statutory inspections during the remainder of 2013-14.

Exception noted under criterion 1

Application made to extend an already expired warrant

Section 19(1) of the Act enables a law enforcement officer, to whom a surveillance device has been issued, to apply for an extension of a warrant at any time before the expiry of the warrant.

For one warrant an application to extend the warrant was made, and subsequently granted, despite the warrant having already expired.

In response to this issue, the AFP advised that its internal guidance and training has been reinvigorated to clearly inform its officers of the provisions under s 19 of the Act.

Exception noted under criterion 2

Record of details of tracking device authorisations to be kept

Section 40(1)(f) and (g) of the Act requires that the written record of a tracking device authorisation state the vehicle on which the use of a tracking device is authorised and the name of the person on whom the use of a tracking device is authorised.

For one authorisation, the written record did not state these details. The AFP noted this finding and advised that subsequent to the inspection the written record was amended, with the endorsement of the authorising officer, to include the missing details.

Exceptions noted under criterion 3 (including where we were unable to determine compliance)

Use of devices without the authority of a warrant

As the AFP did not immediately identify that it had applied to extend an already expired warrant (as discussed above), surveillance activities occurred on three occasions without the authority of a warrant.

In response to this issue, the AFP advised that it has quarantined all protected information obtained from the use of devices after the expiry of the related warrant.

Access to records to confirm lawful access to premises under 'person warrants'

For six person warrants, there was insufficient information to establish a link between the person named on the warrant and all the premises or locations where the device/s were installed or used. As a consequence we were unable to verify compliance with s 18(2)(c)(i) for these warrants at the inspection (see page 4 for the Act's requirements relating to person warrants).

As previously stated, this is not the first time that this issue has been identified at the AFP.

Subsequent to the inspection, the AFP advised that for two warrants, it had sought confirmation from investigators that the devices were used and/or installed in premises and locations where the person named on the warrant was reasonably believed to be.

In relation to the remaining four warrants, the AFP advised that it considered the use of devices recorded on file to be consistent with information provided in the relevant affidavit.

We are of the view that a contemporaneous record made at the time a device is used is the best form of evidence to demonstrate that actions were undertaken in accordance with the authority of a warrant. The information provided within an affidavit may establish the rationale behind investigators using a device, but it does not always confirm that a connection existed between the premises at which a device was used and the person named on the warrant, at the time the device was used.

We suggested that the AFP implement procedures to ensure that contemporaneous records are kept in relation to each use of a device under a 'person warrant', to demonstrate a link between where the device was used and the location where it was reasonably believed that the person named on the warrant would be.

Subsequent to the inspection, the AFP advised that procedures will be implemented to ensure information is collected contemporaneously to demonstrate this link.

Progress made since previous report

In our last report to the Attorney-General, we noted that the AFP did not comply with all of the requirements of the Act relating to extraterritorial surveillance and a recovery order. As the AFP did not apply any of the relevant provisions during this inspection period, no assessment of the AFP's progress in addressing these issues could be made.

CRIME AND MISCONDUCT COMMISSION

Inspection results

Criteria	Assessment
1. Were applications for warrants and authorisations properly made?	Compliant.
2. Were authorisations properly issued?	N/A
3. Were surveillance devices used lawfully?	N/A
4. Were revocations of warrants properly made?	N/A
5. Were records properly kept by the agency?	Compliant.
6. Were reports properly made by the agency?	Compliant.
7. Was protected information properly dealt with by the agency?	Nothing to indicate otherwise.

No issues were identified and no recommendations were made as a result of the inspection carried out in August 2013.

Progress made since previous report

There were no issues identified in our last report to the Attorney-General which required follow-up.

NEW SOUTH WALES POLICE FORCE

Inspection results

Criteria	Assessment
1. Were applications for warrants and authorisations properly made?	N/A
2. Were authorisations properly issued?	N/A
3. Were surveillance devices used lawfully?	N/A
4. Were revocations of warrants properly made?	N/A
5. Were records properly kept by the agency?	N/A
6. Were reports properly made by the agency?	N/A
7. Was protected information properly dealt with by the agency?	Compliant[4].

No issues were identified and no recommendations were made as a result of the inspection carried out in September 2013.

Progress made since previous report

In our report to the Attorney-General provided in September 2013 we reported that the NSW Police Force was not compliant with s 46(1)(b) of the Act, which relates to the destruction and retention of protected information obtained as a result of using surveillance devices. However, we were satisfied that it had implemented procedures to address this issue.

At this inspection we confirmed that these measures have been effective.

[4] This finding of compliant is equivalent to 'nothing to indicate otherwise'.

VICTORIA POLICE

Inspection results

Criteria	Assessment
1. Were applications for warrants and authorisations properly made?	Compliant.
2. Were authorisations properly issued?	N/A
3. Were surveillance devices used lawfully?	Nothing to indicate otherwise
4. Were revocations of warrants properly made?	Compliant.
5. Were records properly kept by the agency?	Compliant.
6. Were reports properly made by the agency?	Compliant.
7. Was protected information properly dealt with by the agency?	Nothing to indicate otherwise.

No issues were identified and no recommendations were made as a result of the inspection carried out in September 2013.

Progress made since previous report

There were no issues identified in our report to the Attorney-General provided in March 2013 which required follow-up.

Colin Neave
Commonwealth Ombudsman