

**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 2013

**AUSTRALIAN COMMISSION FOR LAW ENFORCEMENT
INTEGRITY**

Records from 1 January to 30 June 2012

AUSTRALIAN CRIME COMMISSION
Records from 1 January to 30 June 2012

AUSTRALIAN FEDERAL POLICE
Records from 1 January to 30 June 2012

NEW SOUTH WALES POLICE FORCE
Records from 1 July 2011 to 31 August 2012

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

September 2013

**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 2013

**AUSTRALIAN COMMISSION FOR LAW ENFORCEMENT
INTEGRITY**

Records from 1 January to 30 June 2012

AUSTRALIAN CRIME COMMISSION
Records from 1 January to 30 June 2012

AUSTRALIAN FEDERAL POLICE
Records from 1 January to 30 June 2012

NEW SOUTH WALES POLICE FORCE
Records from 1 July 2011 to 31 August 2012

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

September 2013

ISSN 1833-9263

© Commonwealth of Australia 2013

Ownership of intellectual property rights in this publication

Unless otherwise noted, copyright (and any other intellectual property rights, if any) in this publication is owned by the Commonwealth of Australia (referred to below as the Commonwealth).

Creative Commons licence

With the exception of the Coat of Arms (see below) this publication is licensed under a Creative Commons Attribution 3.0 Australia Licence.



Creative Commons Attribution 3.0 Australia Licence is a standard form licence agreement that allows you to copy, distribute, transmit and adapt this publication provided that you attribute the work. A summary of the licence terms is available from <http://creativecommons.org/licenses/by/3.0/au/deed.en>. The full licence terms are available from <http://creativecommons.org/licenses/by/3.0/au/legalcode>.

The Commonwealth's preference is that you attribute this publication (and any material sourced from it) using the following wording:

Source: Licensed from the Commonwealth Ombudsman under a Creative Commons Attribution 3.0 Australia Licence.

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are set out on the It's an Honour website at www.itsanhonour.gov.au.

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.....	1
INSPECTION OBJECTIVE AND SCOPE	2
SUMMARY OF INSPECTION RESULTS	3
AUSTRALIAN COMMISSION FOR LAW ENFORCEMENT INTEGRITY	5
Inspection results.....	5
AUSTRALIAN CRIME COMMISSION.....	6
Inspection results.....	6
Progress made since previous report	6
Issues arising from the inspection.....	7
AUSTRALIAN FEDERAL POLICE.....	9
Inspection results.....	9
Progress made since previous report	9
Issues arising from the inspection.....	10
NEW SOUTH WALES POLICE FORCE	13
Inspection results.....	13
Progress made since previous report	13
Issue arising from the inspection	13

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.

Section 55(1) of the Act requires the Commonwealth 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 Crime Commission (ACC), the Australian Federal Police (AFP), the Australian Commission for Law Enforcement Integrity (ACLEI), police forces of each state and territory, such as the New South Wales Police Force (NSW Police Force), and other specified state and territory law enforcement agencies.

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).

Report to the Attorney-General on the results of inspections of records under s 55 of the *Surveillance Devices Act 2004*, September 2013

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

Table 1. Inspections finalised between 1 January and 30 June 2013

Agency	Records covered by the inspection period	Dates of inspection	Finalised
			Report to the agency completed
ACLEI	1 January to 30 June 2012	28 November 2012	26 March 2013
ACC	1 January to 30 June 2012	23 to 25 October 2012	6 February 2013
AFP	1 January to 30 June 2012	3 to 5 September 2012	3 January 2013
NSW Police Force	1 July 2011 to 31 August 2012	22 October 2012	12 February 2013

Detailed internal reports on the results of each inspection were provided to each agency. This report summarises the results of these inspections, outlining any significant compliance and administrative issues.

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?
2. Were warrants and authorisations properly issued?
3. Were surveillance devices used lawfully?
4. Were revocations of warrants properly made?
5. Were records properly kept and used by the agency?
6. Were reports properly made by the agency?
7. Was protected information properly dealt with by the agency?

Criterion 7 is a new addition since our previous report. It reflects our assessment of agencies' compliance with the Act in relation to dealing with

protected information². This aspect of our inspection was previously included under criterion 6.

All records held by each agency 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 period.

SUMMARY OF INSPECTION RESULTS

Table 2. Summary of inspection results

Criteria	ACLEI	ACC	AFP	NSWPF
1. Were applications for warrants and authorisations properly made?	Compliant	Compliant	Compliant with administrative issues noted	N/A
2. Were warrants and authorisations properly issued?	Compliant	Compliant with administrative issues noted	Compliant with an administrative issue noted	N/A
3. Were surveillance devices used lawfully?	Nothing to indicate otherwise	Nothing to indicate otherwise	Compliant with exceptions Recommendation made	N/A
4. Were revocations of warrants properly made?	N/A	Compliant with administrative issues noted	Compliant	N/A
5. Were records properly kept and used by the agency?	Compliant, except for one instance	Compliant	Compliant	N/A
6. Were reports properly made by the agency?	Compliant	Compliant with administrative issues noted	Compliant with an administrative issue noted	N/A
7. Was protected information properly dealt with by the agency?	Nothing to indicate otherwise	Compliant with exceptions	Compliant with exceptions	Not compliant in 40 instances

² Section 44(1) of the Act broadly defines protected information to mean any information obtained from the use of a surveillance device under a warrant, an emergency authorisation or a tracking device authorisation.

Report to the Attorney-General on the results of inspections of records under s 55 of the *Surveillance Devices Act 2004*, September 2013

The majority of issues identified at our inspections were administrative in nature. The ACC self-disclosed most of its issues prior to the inspection.

We made one recommendation to the AFP, regarding the need to ensure that surveillance devices are used and retrieved in accordance with legislative requirements.

The report discusses issues we noted at the ACC, the AFP and the NSW Police Force relating to the destruction and retention of protected information. We have been advised that all three agencies have implemented procedural changes to ensure that they meet the relevant requirements of the Act.

All four agencies displayed a positive attitude towards compliance and are responsive to addressing the issues identified as a result of our inspections.

AUSTRALIAN COMMISSION FOR LAW ENFORCEMENT INTEGRITY

Inspection results

The inspection of ACLEI's surveillance device records was conducted on 28 November 2012. The inspection examined one surveillance device warrant (and associated records) that expired during the period 1 January to 30 June 2012. A report of this inspection was provided to ACLEI on 26 March 2013.

This was the first time we had inspected the surveillance device records of ACLEI and it was assessed as compliant with the Act with a minor exception relating to record keeping which was subsequently amended. No other issues were identified and no recommendations were made as a result of the inspection.

In relation to ACLEI's application process, we noted its good practice of attaching relevant internal authorisations, providing assurance to the issuing authority that the applicant is authorised to apply for the warrant.

AUSTRALIAN CRIME COMMISSION

Inspection results

The inspection of the ACC's records was conducted from 23 to 25 September 2012. The inspection examined surveillance device warrants and tracking device authorisations (and associated records) that expired or were revoked during the period 1 January to 30 June 2012, and also records relating to the destruction and retention of protected information. A report of the results of this inspection was provided to the ACC on 6 February 2013.

We inspected records relating to: 53 warrants and authorisations (a 100% sample); the destruction of protected information obtained under 19 warrants and authorisations (a 100% sample); and the retention of protected information obtained under 11 warrants and authorisations (a 100% sample).

The ACC was assessed as compliant with the Act except for one warrant where protected information was destroyed without evidence that the chief officer was satisfied that it was no longer required; and four instances where protected information was destroyed or retained more than five years after the information was made, without certification by the chief officer. No recommendations were made as a result of the inspection.

Progress made since previous report

As noted in our last report to the Attorney-General, the ACC self-disclosed that protected information obtained under 15 warrants and tracking device authorisations was retained for more than five years without the chief officer's certification as required under s 46(1)(b)(ii) of the Act. This issue was also reported to the Attorney-General in September 2012 in relation to 22 warrants.

The ACC has advised that it has now considered all protected information made from 2004 to 2007, ensuring this information is either destroyed or retained with the chief officer's certification. As a result of finalising this review, the ACC has identified an additional number of records where protected information was destroyed and or retained more than five years after the information was made without the chief officer's certification. This issue is further discussed below.

We also noted in our last report, four instances where there were insufficient records available to determine whether verbal applications for tracking device authorisations met the requirements of section 14(5)(a)(ii) of the Act. No further instances were noted at this inspection.

Issues arising from the inspection

Protected information was destroyed without the chief officer's certification

Under s 46(1)(b), as soon as practicable after a record or report comprising protected information is made, the chief officer must ensure that the record or report is destroyed if the chief officer is satisfied that it is no longer required by the law enforcement agency. Therefore, the chief officer is required to consider whether or not protected information is still required before it can be destroyed. We are of the view that this consideration is best recorded in writing.

The ACC self-disclosed that protected information under one warrant was destroyed before obtaining the chief officer's authorisation. The ACC advised that this occurred because the information was not considered relevant to the investigation.

The ACC sought internal legal advice which confirmed that the chief officer's authorisation was required before the information could be destroyed. The ACC also raised this issue with the Attorney-General's Department.

To avoid similar situations in the future, the ACC advised that it has updated its training, informed relevant team managers and the national manager of this issue, and has provided specific guidance in its standard operating procedures.

Destruction and retention of protected information

Under s 46(1)(b), the decision to retain or destroy protected information must be made within five years after its creation. If the chief officer decides to retain protected information, the chief officer must certify to that effect within the five years, and every five years thereafter, until the protected information is destroyed.

The ACC self-disclosed that protected information obtained under two warrants and one tracking device authorisation was destroyed more than five years after the information was made, and there was no certification from the chief officer to retain this information.

We also noted that the chief officer's certification to retain protected information under a further warrant was not provided within five years after the protected information was made.

Report to the Attorney-General on the results of inspections of records under s 55 of the *Surveillance Devices Act 2004*, September 2013

As noted previously, the ACC has advised that it has now considered all protected information made from 2004 to 2007, ensuring this information is either destroyed or retained with the chief officer's certification.

AUSTRALIAN FEDERAL POLICE

Inspection results

The inspection of the AFP's records was conducted from 3 to 5 September 2012. The inspection examined surveillance device warrants and tracking device authorisations (and associated records) that expired or were revoked during the period 1 January to 30 June 2012 and also records relating to the destruction and retention of protected information. A report of the results of this inspection was provided to the AFP on 3 January 2013.

We inspected records relating to: 72 warrants and authorisations (a 27% sample); the destruction of protected information obtained under 70 warrants and authorisations (a 37% sample); and the retention of protected information obtained under 59 warrants and authorisations (a 61% sample).

The AFP was assessed as compliant with the Act except for three instances where surveillance devices had been used or may have been used without lawful authority. As a result one recommendation was made. Additionally, there were at least 30 instances where protected information was destroyed or retained more than five years after the information was made, without certification by the chief officer.

Progress made since previous report

As noted in our last report to the Attorney-General, the AFP was assessed as compliant with the requirements of the Act except in two cases where there was a delay in notifying the Attorney-General of extraterritorial surveillance activities; and the destruction requirements under s 46(1)(b) were not met. The first issue was not noted again at this inspection. The second issue relating to the destruction and retention of protected information was noted again at this inspection due to the AFP finalising its review of old records.

The AFP advised that it had implemented procedures in June 2012 for the regular review of protected information to ensure that protected information is destroyed if it is no longer required. If protected information is required to be kept for longer than five years after it is made, the AFP also has procedures to obtain a certification from the chief officer (or a delegate) in accordance with s 46(1)(b).

At this inspection, the destruction and retention of records we inspected predated the AFP's new procedures. Therefore, we noted a number of records containing protected information that were not destroyed or certified to be

retained within five years after they had been made. This issue is further discussed below.

Issues arising from the inspection

Use and retrieval of surveillance devices outside the period of validity of tracking device authorisations and warrants

The AFP self-disclosed three instances where surveillance devices had been used or may have been used without lawful authority.

The first instance involved a tracking device being retrieved two days after the expiry of the warrant. The AFP advised that this was due to a miscalculation of the expiry date of the warrant.

The second instance related to the AFP retrieving a tracking device before the relevant tracking device authorisation was issued.

Under s 39(6) of the Act, an appropriate authorising officer may authorise the retrieval of a tracking device without a warrant, if the retrieval does not involve entry onto premises. The AFP retrieved a tracking device from a vehicle one day prior to the granting of the retrieval authorisation. As a consequence, the retrieval of this tracking device was conducted without lawful authority.

The third instance related to the AFP using a tracking device before the relevant tracking device authorisation was issued.

Section 39(1) of the Act does not allow the use of a tracking device without a warrant unless there is written permission from an appropriate authorising officer. While the Act allows a verbal application to be made, it requires a written authorisation before a law enforcement officer can use tracking devices without a warrant.

The AFP advised that a tracking device was installed on the same day that a 'verbal authorisation' was provided. There was no record of the verbal application or approval available at the inspection. The written authorisation was provided the day after the device was installed. In our view, the AFP may not have complied with s 39(1) because the installation of the tracking device did not occur under written permission.

The AFP advised that no protected information had been obtained by the use of surveillance devices under this tracking device authorisation.

It is important that AFP officers are aware of the requirements of the Act in relation to the lawful use of surveillance devices, particularly when they are used under a tracking device authorisation granted internally. Operational decisions should only be taken with a clear understanding of the legislative requirements. As a consequence, we made the following recommendation to the AFP.

Recommendation

That the Australian Federal Police provides or strengthens guidance to those who are responsible for the use and retrieval of surveillance devices on the legislative requirements relating to their use and retrieval; this guidance may include examples of particular situations and the application of the *Surveillance Devices Act 2004* to these situations

In response to this recommendation, the AFP advised that a decision matrix has been developed to provide clear guidance to AFP members regarding the legislative requirements and training will also be conducted. We will assess the effectiveness of these measures in future inspections.

Destruction and retention of protected information

As detailed previously for the ACC on page 7, s 46(1)(b) of the Act imposes requirements on how law enforcement agencies destroy or retain protected information.

We identified that protected information obtained under 29 warrants was destroyed more than five years after the information had been made; and the AFP did not have certification from the chief officer to retain this information.

The protected information obtained under these 29 warrants was destroyed as a result of the AFP completing the review of its existing holdings of protected information after we identified this issue at a previous inspection.

The AFP later advised that an exemption under s 46(3) applied to two of the 29 warrants so that the requirements under s 46(1) did not apply. Section 46(3) of the Act provides that s 46(1) does not apply to a record or report comprising protected information that was received into evidence in legal proceedings or disciplinary proceedings.

We also identified that the chief officer's certification to retain protected information under 43 warrants was not provided within five years after the

Report to the Attorney-General on the results of inspections of records under s 55 of the *Surveillance Devices Act 2004*, September 2013

protected information was made. The AFP advised that the exemption under s 46(3) applied to 40 of these warrants.

NEW SOUTH WALES POLICE FORCE

Inspection results

The inspection of the NSW Police Force's records was conducted on 22 October 2012. The inspection examined records relating to the retention and destruction of protected information obtained under 54 surveillance device warrants and tracking device authorisations (a 100% sample). The retention and destruction processes were undertaken during the period 1 July 2011 to 31 August 2012. The NSW Police Force advised that no warrants or tracking device authorisations expired or were revoked during the inspection period. A report of the results of this inspection was provided to the NSW Police Force on 12 February 2013.

Progress made since previous report

In our report provided to the Attorney-General in September 2012, we made a recommendation that the NSW Police Force should implement procedures to fulfil the requirements of s 46(1)(b) of the Act, relating to the retention and destruction of protected information obtained under surveillance device warrants and tracking device authorisations.

The NSW Police Force agreed to this recommendation and updated its Standard Operating Procedures to include managing protected information in accordance with the Act. This included establishing a Review Register, which identifies under which warrants and authorisations protected information was obtained, and Destruction and Retention Registers for the management of protected information.

The NSW Police Force also advised that it has reviewed its holdings of protected information and sought the chief officer's certification to retain or destroy the protected information. We commend the NSW Police Force for the way in which it has addressed these issues and will continue to monitor its progress.

Issue arising from the inspection – destruction and retention of protected information

As discussed above, the NSW Police Force had not previously reviewed its holdings of protected information for destruction or retention in accordance with the Act. The NSW Police Force advised that protected information was obtained under warrants and authorisations issued during the 2004-05, 2005-06 and 2006-07 financial years.

Report to the Attorney-General on the results of inspections of records under s 55 of the *Surveillance Devices Act 2004*, September 2013

Therefore, protected information obtained under 40 out of 54 warrants and authorisations was retained for a period longer than five years without the chief officer's certification, contrary to s 46(1)(b) of the Act. Since our inspection, the majority of this protected information has been formally destroyed or retained, but not within the legislative timeframe.

We are satisfied that the NSW Police Force has implemented procedures to address the requirements of s 46 in the future.

Colin Neave
Commonwealth Ombudsman

