COMMONWEALTH OMBUDSMAN

Report to the Attorney-General on agencies' compliance with the *Surveillance Devices Act 2004*

For the period 1 July to 31 December 2015

AUSTRALIAN COMMISSION FOR LAW ENFORCEMENT INTEGRITY
Records from 1 July to 31 December 2014

AUSTRALIAN CRIME COMMISSION
Records from 1 July to 31 December 2014

AUSTRALIAN FEDERAL POLICE
Records from 1 July to 31 December 2014

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

March 2016

COMMONWEALTH OMBUDSMAN

Report to the Attorney-General on agencies' compliance with the *Surveillance Devices Act 2004*

For the period 1 July to 31 December 2015

AUSTRALIAN COMMISSION FOR LAW ENFORCEMENT INTEGRITY
Records from 1 July to 31 December 2014

AUSTRALIAN CRIME COMMISSION
Records from 1 July to 31 December 2014

AUSTRALIAN FEDERAL POLICE
Records from 1 July to 31 December 2014

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

March 2016

ISSN 2204-4027

Contact us
Inquiries regarding the licence and any use of this report are welcome at:

Commonwealth Ombudsman
Level 5, 14 Childers Street
Canberra ACT 2600
Tel: 1300 362 072
Email: ombudsman@ombudsman.gov.au

CONTENTS

INTRODUCTION

The *Surveillance Devices Act 2004* (the Act) establishes procedures for law enforcement officers to obtain warrants, emergency authorisations and tracking device authorisations for the installation and use of surveillance devices.[1]

Surveillance devices may be used in relation to criminal investigations and the location and safe recovery of children.

The Act allows certain surveillance activities to be conducted either under a warrant (issued by an eligible Judge or nominated Administrative Appeals Tribunal member), by an internally issued authorisation or without formal authority.

The use, communication and publication of information obtained through the use of surveillance devices or that is otherwise connected with surveillance device operations is restricted by the Act.

The Act imposes requirements for the secure storage and destruction of records, and the making of reports, in connection with surveillance device operations. It also imposes reporting obligations on law enforcement agencies to ensure an appropriate level of transparency.

What we do

The Commonwealth Ombudsman (the Ombudsman) performs the independent oversight mechanism included in the Act. The Ombudsman is required to inspect the records of law enforcement agencies that used surveillance devices to determine their compliance with the Act and report the results to the Commonwealth Attorney-General every six-months.

This report sets out the results of our inspections finalised between 1 July and 31 December 2015.

Why we oversee agencies

The use of surveillance devices is one of the most intrusive covert powers afforded to law enforcement agencies. Part of the

[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).

Ombudsman's role is to provide assurance to the Attorney-General and the public that agencies are using their powers as Parliament intended, and if not, hold the agencies accountable.

How we oversee agencies

We have developed a set of inspection methodologies that we apply consistently across all agencies. These methodologies are based on legislative requirements and best-practice standards in auditing, and ensure the integrity of each inspection.

We focus our inspections on areas of high risk and take into consideration the impact of non-compliance; for example, unnecessary privacy intrusion.

We form our assessments based on the records made available at the inspection, discussions with relevant teams, processes we observe and information staff provide in response to any identified issues. To ensure that agencies are aware of what we will be assessing, we provide them with a broad outline of our criteria prior to each inspection. This assists the agency to identify sources of information to demonstrate compliance. We can rely on coercive powers to obtain any information relevant to the inspection if necessary.

We also encourage agencies to be upfront and self-disclose any instances of non-compliance to our office and inform us of any remedial action the agency has taken.

At the end of each inspection we provide our preliminary findings to the agency to enable the agency to take any immediate remedial action.

We may also assist agencies in ensuring compliance through assessing agencies' policies and procedures, communicating 'best-practices' in compliance, and engaging with agencies outside of the inspection process.

Our criteria

The objective of our inspections is to determine the extent of compliance with the Act by the agency and its law enforcement officers, and we use the following criteria to assess compliance.

1. Were applications for warrants and authorisations properly made?
2. Were authorisations properly issued?

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

Appendix A provides further details on our criteria.

How we report

After an inspection, agencies are provided with detailed inspection reports. To ensure procedural fairness we provide a draft report on our findings to the agency for comment before it is finalised. The finalised reports are desensitised and form the basis of this six-monthly report to the Attorney-General. Inspection results are considered finalised once the Ombudsman's internal report to the agency is completed, so typically there will be some delay between the date of inspection and the report to the Attorney-General.

Included in this report is: an overview of our inspection findings across each agency; a discussion of each agency's progress in addressing any significant findings from the previous inspection; and details of any significant issues resulting from the inspections.

We may also discuss issues other than instances of non-compliance, such as the adequacies of an agency's policies and procedures to ensure compliance with the Act. Examples of what we may not include in this report are administrative issues or instances of non-compliance where the consequences are negligible, for example, when actions did not result in unnecessary privacy intrusion.

Relevant agencies

This report includes the results of our inspections of the Australian Commission for Law Enforcement Integrity (ACLEI), the Australian Crime Commission (ACC) and the Australian Federal Police (AFP).

Inspection findings overview

The following table provides an overview of inspection findings across each agency.[2]

[2] This table provides a comprehensive overview of all inspection findings. These may not all be included in the body of this report as they may, for example, be administrative issues or instances of non-compliance where the consequences are negligible.

Agency	Australian Commission for Law Enforcement Integrity	Australian Crime Commission	Australian Federal Police
Inspection period[3]	1 July to 31 December 2014	1 July to 31 December 2014	1 July to 31 December 2014
Number of records inspected	6/6 warrants	62/136 (total warrants) 62/70 executed warrants 14/55 destructions 6/9 tracking device authorisations	86/342 (total warrants) 76/151 executed warrants 35/204 destructions 24/30 retentions
Criteria	***Inspection findings***		
1. Were applications for warrants and authorisations properly made?	Compliant with two administrative issues noted.	Compliant except in two instances where we were unable to determine compliance.	Compliant with four exceptions. Unable to determine compliance in two instances.
2. Were authorisations properly issued?	No authorisations were issued during the inspection period.	Compliant.	Compliant.
3. Were surveillance devices used lawfully?	Unable to determine compliance in one instance.	Nothing to indicate otherwise.	Nothing to indicate otherwise except in five instances.
4. Were revocations of warrants properly made?	Compliant.	Compliant.	Compliant with three exceptions.
5. Were records properly kept by the agency?	Compliant.	Compliant.	Compliant with two exceptions.
6. Were reports properly made by the agency?	Compliant except in one instance.	Compliant.	Compliant with three exceptions.
7. Was protected information properly dealt with by the agency?	Nothing to indicate otherwise.	Nothing to indicate otherwise except in three instances.	Nothing to indicate otherwise except in 16 instances. Unable to determine compliance in four instances.

[3] Inspection period refers to the period during which warrants and authorisations either expired or were revoked.

FINDINGS

AUSTRALIAN COMMISSION FOR LAW ENFORCEMENT INTEGRITY

We conducted an inspection at ACLEI on 10 and 11 February 2015 in Canberra. Although no recommendations were made as a result of the inspection, we were unable to determine compliance in one instance, which is further discussed below. We would like to acknowledge ACLEI's cooperation during the inspection.

Issues from previous inspections

Although no recommendations were made as a result of the previous inspection in September 2014, one issue was identified that again was relevant to the February 2015 inspection.

This issue related to the use of a surveillance device on a portable object. The warrant for this device permitted its use at a premises where the person listed on the warrant was reasonably believed to be or likely to be (s 18(2)(c)(i)). We were unable to determine whether this was the case here, although the portable object was identified as being used by the person listed on the warrant.

We suggested to ACLEI that, in such cases, it consider applying for a warrant in respect of both the person and the portable object. Or, if it is not known what portable objects are being used by the person (at the time the warrant is sought), apply for a variation to the warrant (under s 19) to include the object, once it becomes known.

In response to this issue, ACLEI advised that it would consider our suggestion, and in this instance, it had a concurrent warrant obtained under different legislation from which it could confirm lawful use of the device.

We accepted this advice, but it was not confirmed at the February 2015 inspection.

Inspection findings

In addition to the finding below, we noted administrative issues around its applications to extend warrants, which had effected its reporting requirements under s 49 regarding extensions. However, as a result of our office raising this with ACLEI, it advised that its internal

processes have been strengthened to provide assurance that the correct legislative references are applied. We acknowledge the remedial action undertaken by ACLEI.

Finding 1: Use of a surveillance device on a portable object

What the Act allows

Section 18(1)(c) of the Act 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. Section 18(2)(c)(i) states that this type of warrant authorises the installation, use and maintenance of devices on premises where the person is reasonably believed to be or likely to be. Therefore, where surveillance devices have been installed under this type of warrant we would expect to see the information that connects the location where a device has been used to the person named on the warrant.

What we found

For one warrant, based on the information ACLEI provided our office at the inspection, we were unable to conclusively determine that a portable object, on which a surveillance device was installed and used, was located in a premises that was connected to the person named on the warrant. Therefore we were unable to determine compliance with s 18(1)(c).

Suggested practice

We reiterated our suggestion to ACLEI that it could demonstrate compliance by either applying for a warrant in respect of both the person and the portable object or applying a variation to the warrant under section 19.

We also suggested that ACLEI could demonstrate compliance by providing our office with information about its processes in these instances.

AUSTRALIAN CRIME COMMISSION

We conducted an inspection at the ACC from 17 to 19 March 2015 in Brisbane. Although no recommendations were made as a result of this inspection, we were unable to determine compliance in two instances following self-disclosures from the ACC, which are further discussed below. The ACC also disclosed one instance where it could not be confirmed whether protected information obtained from surveillance devices was kept securely. However, we are satisfied that the ACC has taken self-initiated measures to address these issues.

We would also like to acknowledge the ACC's cooperation during the inspection and for its ongoing frank and open engagement with our office.

Issues from previous inspections

During the March 2015 inspection we re-examined an issue from a previous inspection conducted in September 2013[4], where the ACC self-disclosed that protected information that it destroyed had been recovered for continued use.

As we consider protected information to be destroyed once it is rendered unrecoverable, we requested further information about the recovery of deleted protected information. The ACC advised that all electronic records are retained for up to seven years to ensure compliance with the *Archives Act 1983* and to minimise the corporate risk of lost data. The ACC also advised of several practical difficulties in excluding protected information from this practice in order to deem it unrecoverable. The ACC advised that deleted information can be recovered by system administrators; however its internal policy is only to do so with appropriate approval.

We noted the practical difficulties of destroying (rendering unrecoverable) protected information and did not suggest any changes to practices in this regard. However, to meet the Act's intention, we suggested that the ACC change its policy so that it does not permit the recovery of protected information once it has been deleted.

The ACC agreed with this suggestion and advised that it will update its procedures and guidelines accordingly. It further advised that

[4] The results of this inspection are available here: http://www.ombudsman.gov.au/__data/assets/pdf_file/0028/29359/September-2014-Report-to-the-Attorney-General-on-the-results-of-inspections-of-records-under-s-55-of-the-Surveillance-Devices-Act-2004.pdf

officers who authorise the destruction of protected information will be reminded of this policy in all correspondence.

Inspection Findings

In addition to the below findings, the ACC self-disclosed that not all protected information had been destroyed within five years of its creation, contrary to s 46(1)(b). We note that the majority of the protected information obtained under these warrants had been destroyed within the five year period and that these instances were most likely identified as a result of the ACC's forensic auditing of its destruction processes.

Finding 1: Unable to determine if oral applications for a tracking device were properly made

What the Act allows

Section 39(9)(b) of the Act provides that an (internal) application for permission to use a tracking device must address the matters that would be required to be addressed if the law enforcement officer was instead applying to an eligible Judge or nominated Administrative Appeals Tribunal member for a surveillance device warrant. These matters are set out under s 14 of the Act.

An application may be made either in writing or orally. For oral applications, the ACC's usual practice is for investigators to complete a checklist which addresses most of the matters under s 14 at the time of the application and then supplement it with a written application at a later time. The written application usually addresses all of the matters under s 14.

What we found and what was self-disclosed

For two tracking device authorisations the ACC self-disclosed that there was insufficient information available to demonstrate compliance with s 39(9)(b). In both instances, the investigator had made an oral application for the authorisation; however, only the checklist was completed. As a result, we were unable to determine compliance with these provisions.

Additionally, for one of the above instances, the details stated on the oral checklist differed from those reported to the Attorney-General under s 49 of the Act. This raises doubt about the accuracy of these records.

The ACC's advised remedial action

The ACC advised that it has reviewed and updated its procedures for oral applications and now has a more comprehensive checklist in place. The ACC advised that the new checklist addresses the matters under s 14, which eliminates the need for investigators to complete a separate written application.

Finding 2: Unable to ensure protected information was kept securely

What the Act allows

Under section 46(1)(a) the chief officer of a law enforcement agency must ensure that every record comprising protected information is kept in a secure place that is not accessible to people who are not entitled to deal with the record.

Self-disclosed issue

The ACC self-disclosed that two DVD's containing protected information obtained under a warrant could not be accounted for, however, it expects instances like this to be avoided in future, due to its thorough destruction processes.

AUSTRALIAN FEDERAL POLICE

We conducted an inspection at the AFP from 23 to 26 March 2015 in Canberra. Although no recommendations were made as a result of the inspection, a number of issues were identified. We would like to acknowledge the AFP's frank disclosure and assistance it provided during the inspection.

Issues from previous inspections

At the inspection, we examine any progress made by the AFP in relation to previous inspection findings. Two issues which had been identified at previous inspections were again identified at the March 2015 inspection.

The first of these issues related to there being insufficient information available to demonstrate that surveillance devices were used only on premises or at locations where the person named on the warrant was reasonably believed to be. As we had previously reported on this issue a number of times, we sought information from AFP technical specialists regarding their processes, policies and accountability mechanisms when using surveillance devices in these instances. This information was taken into consideration in forming our assessments for the March 2015 inspection and as a result there were significantly fewer instances where we could not determine compliance. This issue is further discussed below under *Finding 3: Surveillance devices used in respect of an unknown person*.

The second issue was an instance where surveillance devices were used outside the authority of a warrant. Although this issue has been previously reported, the circumstances surrounding the instances identified at the March 2015 inspection appear to be different from those previously reported on, and based on the information made available to us, they do not appear systemic in nature. This issue is further discussed below under *Finding 2: Use of surveillance devices outside the authority of the warrant*.

Inspection Findings

In addition to the findings below, we also identified a small number of non-compliances that were administrative in nature.

Finding 1: Use of emergency provisions

What the Act allows

Section 28(1) of the Act states that a law enforcement officer may apply to an appropriate authorising officer for an emergency authorisation for the use of a surveillance device if, in the course of an investigation of a relevant offence, the law enforcement officer reasonably suspects that a number of conditions have been met and it is impracticable to apply for a surveillance device warrant.

What we found

Based on the records available we were unable to determine what offence the AFP was investigating when it applied the emergency authorisation. We also identified that under an emergency authorisation the AFP installed and activated a surveillance device prior to the granting of that authorisation. However, we note the exceptional circumstances of the situation in which these provisions were applied. We also appreciate that this may have been the first time the AFP used these provisions and acknowledge the AFP's frank disclosure and assistance it provided during the inspection when we assessed compliance against these provisions.

The AFP's advised remedial action

The AFP acknowledged the need to develop templates to assist investigators in applying for emergency authorisations, and advised that this body of work is currently being undertaken. The AFP also advised that it conducted a post-activity analysis following the use of a surveillance device prior to the granting of an emergency authorisation. Following this the AFP has advised that it has implemented measures, including greater education regarding emergency authorisations.

Finding 2: Use of surveillance devices outside the authority of the warrant

What the Act allows

Part 5 of the Act sets out the circumstances in which an agency may carry out surveillance activities in a foreign country. Section 18(1)(b) allows for a warrant to be issued in respect of an object of interest and s 18(1)(c) allows for a warrant to be issued in respect of a specified person.

Self-disclosed issue

The AFP self-disclosed that it used surveillance devices on an object while it was located outside of Australia without meeting the requirements of Part 5.

As the warrant authorising the use of these devices was issued under s 18(1)(c), it authorised the use of surveillance devices in respect of a specified person. In this instance it appeared that the AFP had conducted surveillance on the person's partner, which was outside the authority of the warrant.

The AFP's advised remedial action

Once the AFP identified the issue, it advised that it disabled the use of the surveillance devices and quarantined the protected information obtained from the use of the devices. The AFP has since advised that it has continued to review internal processes to ensure that technical areas are made aware of any impending overseas travel so that surveillance devices can be disabled accordingly. The AFP also advised that it will encourage its members to seek warrants in respect of an object, if and when objects of interest are identified.

Finding 3: Surveillance devices used in respect of an unknown person

What the Act allows

Section 18(1)(c) states that a surveillance device warrant may authorise the use of a surveillance device in respect of a specified person or a person whose identity is unknown. Section 18(2)(c)(i) states that this type of warrant authorises the installation, use and maintenance of devices on premises where the person is reasonably believed to be or likely to be.

What we found

In relation to one warrant issued in respect of a person whose identity was unknown, there was insufficient information to demonstrate that all devices were only used on premises where that person was reasonably believed to be or likely to be. Although we could determine the location at which devices were used, we could not establish a link between the location and the unknown person.

In instances where the person's identity is unknown, we cannot rely on our understanding of the AFP's usual practices.

The AFP's advised remedial action

The AFP explained that actions under the warrant had been undertaken and recorded by a state law enforcement agency, which reports in a different format to the AFP. The AFP advised that it will continue to work with investigators to ensure that all relevant information is captured, regardless of different procedures among agencies.

Finding 4: Keeping protected information for longer than five years

What the Act allows

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.

What we found

We identified that protected information obtained under 16 warrants and tracking device authorisations had been kept for a period longer than five years without the chief officer certifying that it could be retained.

What the AFP advised

The AFP advised that protected information is destroyed on an operational basis and regional offices decide whether to commence the AFP's destruction process. If the protected information has not been destroyed and it is approaching the five year period, a reminder is sent that it must either be destroyed or retained. The AFP advised that some of the protected information was destroyed or certified for retention subsequent to the inspection.

Suggested practice

In light of the instances identified at the inspection and it being the responsibility of regional offices to commence destruction processes, the AFP may wish to increase education and awareness in its regional offices as to the destruction requirements of the Act.

APPENDIX A – INSPECTION CRITERIA

1. Were applications for warrants and authorisations properly made?

Under this criterion, we assess agency compliance with the following provisions of the Act:

- making applications for surveillance device warrants under s 14
- making applications for extensions/variations to surveillance device warrants under s 19
- making applications for retrieval warrants under s 22
- making applications for emergency authorisations and subsequent applications to an eligible Judge or a nominated AAT member under ss 28, 29 and 33
- making applications for tracking device authorisations and retrieval of tracking devices under s 39
- keeping each document required by s 51(e) to (h).

2. Were authorisations properly issued?

Under this criterion, we assess agency compliance with the following provisions of the Act:

- written records for emergency authorisations were properly issued under s 31 and each written record of the authorisation was kept in accordance with s 51(c)
- tracking device authorisations were properly issued under ss 39 and 40, and each written record of the authorisation was kept in accordance with s 51(d)
- authorisations for the retrieval of tracking devices were properly issued under ss 39 and 40.

3. Were surveillance devices used lawfully?

Under this criterion, we assess agency compliance with the following provisions of the Act:

- whether surveillance devices were used in accordance with the relevant warrant (s 18)
- whether surveillance devices were used in accordance with the relevant emergency authorisation (ss 18 and 32)
- whether retrieval of surveillance devices or tracking devices was carried out lawfully (ss 26 and 39(11))
- whether tracking devices were used in accordance with the relevant tracking device authorisation (s 39)
- whether extra-territorial surveillance was carried out lawfully (s 42).

4. Were revocations of warrants properly made?

Under this criterion, we assess agency compliance with the following provisions of the Act:

- revoking warrants under ss 20, 21 and 27 and
- keeping records of revocation under s 51(b).

5. Were records properly kept by the agency?

Under this criterion, we assess agency compliance with the following provisions of the Act:

- keeping the register under s 53
- keeping each warrant under s 51(a)
- keeping evidentiary certificates under s 51(k)
- keeping documents under s 52(1)(a) – (d).

6. Were reports properly made by the agency?

Under this criterion, we assess agency compliance with the following provisions of the Act:

- reporting to the Attorney-General under s 49 after the warrant ceased to be in force and keeping each report under s 51(j)
- reporting annually to the Attorney-General under s 50.

7. Was protected information properly dealt with by the agency?

Under this criterion, we assess the agency's compliance with the following provisions of the Act:

- dealing with protected information under ss 46(1)(a) and 52(1)(e) to (h)
- destroying and retaining protected information under ss 46(1)(b) and 52(1)(j).