COMMONWEALTH OMBUDSMAN

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

For the period 1 July to 31 December 2017

AUSTRALIAN COMMISSION FOR LAW ENFORCEMENT INTEGRITY
Records from 1 July to 31 December 2016

AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION
Records from 1 July to 31 December 2016

AUSTRALIAN FEDERAL POLICE
Records from 1 July to 31 December 2016

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

March 2018

COMMONWEALTH OMBUDSMAN

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

For the period 1 July to 31 December 2017

AUSTRALIAN COMMISSION FOR LAW ENFORCEMENT INTEGRITY
Records from 1 July to 31 December 2016

AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION
Records from 1 July to 31 December 2016

AUSTRALIAN FEDERAL POLICE
Records from 1 July to 31 December 2016

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

March 2018

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

OVERVIEW

This report presents the results of inspections conducted by the Commonwealth Ombudsman (the Ombudsman) under s 55 of the *Surveillance Devices Act 2004* (the Act) that were finalised during 1 July to 31 December 2017. This report includes the results of our inspections of the Australian Commission for Law Enforcement Integrity (ACLEI), the Australian Criminal Intelligence Commission (ACIC) and the Australian Federal Police (AFP).

Under the Act, specified law enforcement agencies can covertly use surveillance devices when investigating certain offences. This covert power is given to agencies for the purposes of combating crime and protecting our community.

The Ombudsman provides independent oversight by conducting inspections at each agency that has exercised the surveillance device powers. At these inspections, we assess whether agencies are compliant with the Act, have processes to support compliance, and have used the powers in line with the spirit of the legislation. We also consider agencies' transparency and accountability and encourage agencies to disclose issues to our Office. Where we identify issues, we focus on the actions taken by agencies to address them.

Overall, our inspections found ACLEI, the ACIC and the AFP to be compliant with the requirements of the Act. We identified some exceptions to compliance regarding the AFP's retention of protected information and some minor reporting errors by the ACIC and AFP. We commend the remedial actions taken by agencies to address all issues, including those outstanding from previous inspections.

We note the continued transparency and engagement by agencies with our Office, as evidenced by the disclosure of instances of non-compliance. Furthermore, throughout the inspections, agencies were cooperative and provided access to relevant staff and information. It is evident that agencies are committed to compliance and are receptive to our findings and best practice suggestions.

INTRODUCTION

The Act regulates the use of surveillance devices[1] by law enforcement agencies. Broadly speaking, the Act allows certain surveillance activities to be conducted covertly under a warrant (issued by an eligible Judge or nominated Administrative Appeals Tribunal member), an internally issued authorisation or without formal authority. The Act imposes requirements for the secure storage and destruction of records, and restricts the use, communication and publication of information obtained through the use of surveillance devices.[2] It also imposes reporting obligations on law enforcement agencies to ensure an appropriate level of transparency.

What we do

The Ombudsman performs the independent oversight mechanism included in the Act. The Ombudsman is required to inspect the records of each law enforcement agency to determine the extent of their compliance with the Act and report to the relevant Minister (the Commonwealth Attorney-General) at six-monthly intervals.

Why we oversee agencies

The use of surveillance devices is one of the most intrusive covert powers afforded to law enforcement agencies, and part of the Ombudsman's role is to provide the Minister and the public assurance 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 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, where there is 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

[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] This type of information and records are collectively referred to as 'Protected Information' as defined under s 44 of the Act.

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 agencies to identify sources of information to demonstrate compliance. We can rely on coercive powers to obtain any information relevant to the inspection.

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. Did the agency have the proper authority for the use and/or retrieval of the device?
2. Were surveillance devices used and/or retrieved in accordance with the authority of warrants and authorisations?
3. Is protected information properly stored, used and disclosed?
4. Was protected information properly destroyed and/or retained?
5. Were all records kept in accordance with the Act?
6. Were reports properly made?
7. Was the agency cooperative and frank?

Appendix A provides further details on our inspection criteria and methodology.

How we report

To ensure procedural fairness, agencies were provided with a detailed draft inspection report for comment prior to finalisation. The finalised reports were desensitised and form the basis of this report to the Minister. Inspection results are considered finalised once the Ombudsman's internal report to the agency is completed. As a result, there will typically be some delay between the date of inspection and the report to the Minister.

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

AUSTRALIAN COMMISSION FOR LAW ENFORCEMENT INTEGRITY

We conducted an inspection of ACLEI's surveillance device records on 27 April 2017 for the inspection period 1 July to 31 December 2016.[3] We assessed both surveillance device warrants issued to ACLEI which expired or were revoked during the period and the retention by ACLEI of protected information obtained under four warrants.

We did not assess any tracking device authorisations or destructions of protected information as ACLEI advised no authorisations had expired or were revoked and it did not destroy any protected information during the period.

We did not make any recommendations or suggestions for improvement as a result of the inspection.

We would like to acknowledge ACLEI's cooperation during the inspection and its ongoing frank and open engagement with our Office.

Progress made since the previous inspection

At each inspection, we monitor ACLEI's progress in addressing previous inspection findings. However, this was not necessary on this occasion, as no compliance issues were identified at the previous inspection, which covered records from 1 January to 30 June 2016.

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

AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION

We conducted an inspection of the ACIC's surveillance device records from 28 February to 3 March 2017 for the inspection period 1 July to 31 December 2016. We assessed 63 of the 126 surveillance device warrants issued to, and all 14 tracking device authorisations given by, the ACIC which expired or were revoked during the period. We also assessed the destruction by the ACIC during the period of protected information obtained under three warrants and the retention of protected information obtained under 181 warrants.

We did not make any recommendations as a result of the inspection; however, we identified, and the ACIC self-disclosed, a small number of issues which are discussed below.

We would like to acknowledge the ACIC's cooperation during the inspection and its responsiveness to our inspection findings.

Progress made since the previous inspection

At each inspection, we monitor the ACIC's progress in addressing previous inspection findings. Although we did not make any recommendations as a result of the previous inspection, which covered records from 1 January to 30 June 2016, we were unable to determine compliance in one instance regarding the installation, use and retrieval of a surveillance device. Following that inspection, we sighted additional evidence provided by the ACIC and were satisfied that its actions regarding the surveillance device were lawful.

Inspection findings

Finding 1 – Criterion 2

What the Act requires

Section 18 of the Act provides for the covert use of surveillance devices under a warrant, for the purposes of obtaining protected information.

Self-disclosed non-compliance and remedial action

The ACIC self-disclosed three instances where protected information was obtained without proper authority. In all instances, surveillance devices continued to capture protected information after the relevant warrants had expired.

The ACIC advised that in each instance, it quarantined all protected information captured after the warrants expired.

What we found

In one instance, we were initially unable to determine whether a surveillance device was installed under the authority of a warrant, due to a recording error. The ACIC provided further information subsequent to the inspection which confirmed the installation was conducted lawfully.

Finding 2 – Criterion 4

What the Act requires

Under s 46(1)(b) of the Act, as soon as practicable after a record comprising protected information is created, the chief officer must ensure the record is destroyed if they are satisfied the record is no longer required. The chief officer may decide to retain protected information; however, this decision must be recorded.

The decision to retain or destroy protected information must be made within five years following its creation. If the chief officer decides to retain protected information, the decision must be made every five years until its destruction. Section 46(3) provides an exception to the requirements of s 46 for protected information received into evidence in legal or disciplinary proceedings.

In assessing compliance with s 46(1)(b), we expect agencies to have records indicating:

- evidence the agency has obtained appropriate approval to destroy the protected information;
- evidence the protected information has been destroyed;
- evidence the agency has conducted regular reviews of protected information to assess if it is still required; and
- where protected information is still required after a period of five years, certification from the chief officer (or delegate) that the protected information may be retained (and certification every five year period thereafter).

Self-disclosed non-compliance and remedial action

The ACIC self-disclosed one instance where protected information was destroyed by a partner agency of the ACIC without the approval of either agencies' chief officer (or delegate).

The ACIC also self-disclosed one instance where protected information was transferred to a partner agency and that agency could not account for the location of the protected information. We note the ACIC's attempts to seek confirmation from the partner agency as to the status of the protected information.

In response to these issues, the ACIC advised it will conduct a review of its procedures in relation to partner agencies possessing protected information, to ensure all protected information is accounted for and destroyed appropriately.

Finding 3 – Criterion 6

What the Act requires

Section 49 of the Act sets out the reporting requirements for each warrant issued to, and authorisation given by, an agency. In accordance with s 49, the chief officer must as soon as practicable after a warrant ceases to be in force, provide the Minister with a report, a copy of the warrant and other specified documents. Where a warrant or authorisation is executed, the agency is required to provide additional details in the report to the Minister.

The reporting obligations in the Act are an important transparency and accountability mechanism regarding an agency's covert surveillance device activities.

What we identified and the ACIC's remedial action

In one instance, the ACIC provided a report to the Minister under s 49 which listed a warrant as having not been executed. However, we identified, based on the records made available at the inspection, that a partner agency had executed the ACIC's warrant. The ACIC advised it provided a corrected report to the Minister following the inspection.

AUSTRALIAN FEDERAL POLICE

We conducted an inspection of the AFP's surveillance device records from 14 to 17 March 2017 for the inspection period 1 July to 31 December 2016. We assessed 65 of the 496 surveillance device warrants issued to, and 10 of the 21 tracking device authorisations given by, the AFP which expired or were revoked during the period. We also assessed the destruction by the AFP during the period of protected information obtained under 81 warrants and the retention of protected information obtained under 25 warrants.

We did not make any recommendations as a result of the inspection; however, we identified, and the AFP self-disclosed, a small number of issues which are discussed below.

We would like to acknowledge the AFP's cooperation during the inspection and its responsiveness to our inspection findings.

Progress made since the previous inspection

At each inspection, we monitor the AFP's progress in addressing previous inspection findings. Although we did not make any recommendations as a result of the previous inspection, which covered records from 1 January to 30 June 2016, we identified and the AFP self-disclosed a number of issues. The most significant of these issues related to the use and retrieval of surveillance devices without proper authority, and non-compliance with the destruction and retention provisions.

At this inspection, the AFP self-disclosed one instance where a device was retrieved without proper authority. This issue is discussed in the inspection findings below.

Over the past three years, we have identified ongoing instances of non-compliance by the AFP in relation to the destruction and retention of protected information. The AFP previously advised our Office of a number of remedial actions it has taken to address the issue. This has included the AFP disseminating guidance material to staff and reviewing its current processes. At this inspection, we identified one instance of non-compliance regarding the AFP's retention of protected information. This represents a significant decrease in non-compliance of this nature compared to the previous inspection and indicates the likely effectiveness of the AFP's remedial action. This issue is discussed in the inspection findings below.

Inspection findings

Finding 1 – Criterion 2

What the Act requires

Section 26(1)(a) of the Act states that a retrieval warrant authorises the retrieval of the specific surveillance device stated on the retrieval warrant.

Self-disclosed non-compliance

The AFP self-disclosed one instance where it retrieved a surveillance device under a retrieval warrant from the premises where the device was installed. The type of surveillance device retrieved differed from the device type specified on the retrieval warrant, which the AFP advised was due to an administrative error.

Finding 2 – Criterion 4

What the Act requires

This finding relates to the retaining of protected information by the AFP under s 46 of the Act. The legislative requirements under s 46 are outlined on page 7, under *Finding 2 – Criterion 4*.

What we identified and the AFP's remedial action

We identified one instance where protected information was retained by the AFP for more than five years after it was created, without the authorisation of its chief officer (or delegate). Based on the records made available at the inspection, it appeared the warrant was omitted from the AFP's retention process as a result of an administrative oversight. The AFP advised it has strengthened its retention processes by reviewing the status of protected information more regularly.

Finding 3 – Criterion 6

What the Act requires

This finding relates to the AFP's reporting obligations under s 49 of the Act. The legislative requirements under s 49 are outlined on page 8, under *Finding 3 – Criterion 6*.

What we identified and the AFP's remedial action

In one instance, the AFP provided a report to the Minister under s 49 which listed a warrant as having not been executed. However, we identified, based on the records made available at the inspection, that the AFP had executed the warrant. The AFP advised it provided a corrected report to the Minister following the inspection.

APPENDIX A – INSPECTION CRITERIA AND METHODOLOGY

Inspection focus (1): *Were surveillance devices used in accordance with the Act?*		
Relevant Criteria	**Procedural checks**	**Records-based checks**
1. Did the agency have the proper authority for the use and/or retrieval of the device?	We check the agency has policies and procedures to ensure: – warrants, authorisations, extensions and variations are properly applied for – authorisations are properly granted – extensions and variations are properly sought – warrants are properly revoked.	We inspect applications, warrants, authorisations, variations and other agency records, to assess whether: • applications for surveillance device warrants were made in accordance with s 14 • applications for extensions and/or variations to surveillance device warrants were made in accordance with s 19 • applications for retrieval warrants were made in accordance with s 22 • applications for emergency authorisations and subsequent applications to an eligible Judge or a nominated Administrative Appeals Tribunal member were made in accordance with ss 28, 29, 30 and 33 • written records for emergency authorisations were properly issued in accordance with s 31 • applications for tracking device authorisations and retrieval of tracking devices were made in accordance with s 39 • tracking device authorisations were properly issued in accordance with ss 39 and 40 • warrants were revoked in accordance with ss 20 and 21.

2. Were surveillance devices used and/or retrieved in accordance with the authority of warrants and authorisations?	We check the agency has policies and procedures to ensure: – surveillance devices are used lawfully – it has an auditable system for maintaining surveillance devices – there are sufficient systems in place for capturing the use of surveillance devices – conditions on warrants are adhered to.	We inspect the records and reports relating to the use of surveillance devices against corresponding authorisations and warrants, to assess whether: • use of surveillance devices under a warrant was in accordance with s 18 • use of surveillance devices under an emergency authorisation was in accordance with ss 32 and 18 • retrieval of surveillance devices or tracking devices was carried out in accordance with ss 26 and 39(11) • use of tracking devices under a tracking device authorisation was in accordance with s 39 • any extraterritorial surveillance was in accordance with s 42. In making this assessment, we may also test the veracity of the records by, for example, comparing the details of the records to the information maintained in the systems used by the agency to capture information from surveillance devices. We may also rely on what we understand of an agency's processes and procedures in determining the veracity of such records and take into consideration whether the records were made contemporaneously.

Inspection focus (2): *Is protected information properly managed?*		
Relevant Criteria	**Procedural checks**	**Records-based checks**
3. Is protected information properly stored, used and disclosed?	We check the agency has policies and procedures to ensure: – protected information is kept securely in accordance with the Act – protected information is used and disclosed in accordance with the Act – a person's privacy is protected.	We inspect the records and reports regarding the use and disclosure of protected information that are required under the Act to assess whether anything indicates the agency has used and/or communicated protected information for a purpose other than one outlined in s 45(4).
4. Was protected information properly destroyed and/or retained?	We check the agency has policies and procedures to ensure: – protected information is destroyed in accordance with the Act – protected information is retained in accordance with the Act – protected information is regularly reviewed to assess whether it is still required.	We inspect the records relating to the review, retention and destruction of protected information, including the chief officer's, or delegate's certification that protected information can be retained or destroyed (s 46).

Inspection focus (3): *Was the agency transparent and were reports properly made?*		
Relevant Criteria	**Procedural checks**	**Records-based checks**
5. Were all records kept in accordance with the Act?	We check the agency has policies and procedures to ensure: – it meets its record keeping requirements – it maintains an accurate general register.	We inspect the records presented at the inspection to assess whether the agency has met its record keeping requirements under ss 51 and 52. In assessing whether the agency has met the requirements under s 53 to keep a register of warrants and authorisations, we cross-check the information contained in the register against the corresponding original records.
6. Were reports properly made?	We check the agency has policies and procedures to ensure it accurately reports to the Attorney-General and our Office.	We inspect the copies of reports presented at the inspection to assess whether the agency has met its reporting requirements under ss 49 and 50. In conducting this assessment, we cross-check the information contained in the reports against the corresponding original records.
7. Was the agency cooperative and frank?	Under this criterion we consider: the agency's responsiveness and receptiveness to our inspection findings; whether it has internal reporting mechanisms regarding instances of non-compliance; any self-disclosures the agency may have made to our Office and the Minister; and the agency's overall attitude towards compliance.	