COMMONWEALTH OMBUDSMAN

Report to the Minister for Home Affairs on agencies' compliance with the *Surveillance Devices Act 2004*

For the period 1 July to 31 December 2018

AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION
Records from 1 January to 30 June 2018

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

March 2019

COMMONWEALTH OMBUDSMAN

Report to the Minister for Home Affairs on agencies' compliance with the *Surveillance Devices Act 2004*

For the period 1 July to 31 December 2018

AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION
Records from 1 January to 30 June 2018

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

March 2019

ISSN 2209-752X (Online)
ISSN 2209-7511 (Print)

Contact us
Enquiries 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 the Office of the Commonwealth Ombudsman (the Office) conducted under s 55 of the *Surveillance Devices Act 2004*[1] (the Act), which were finalised between 1 July to 31 December 2018. We conducted one inspection during this period, at the Australian Criminal Intelligence Commission (ACIC).

Under the Act, specified law enforcement agencies can covertly use surveillance devices when investigating certain offences. This power is given to federal agencies for the purposes of combating crime and protecting the community. The Act also allows certain State and Territory law enforcement agencies to use surveillance devices to investigate certain Commonwealth offences and enforce Family Court recovery orders.

The Office provides independent oversight by conducting inspections at each agency that has exercised Commonwealth surveillance device powers during the relevant period. At these inspections, we assess whether agencies were compliant with the Act and had processes in place to support compliance. We also consider agencies' transparency and accountability, and encourage agencies to disclose systemic problems or instances of non-compliance to our Office. Where we have identified problems at previous inspections, we also follow-up on the actions agencies have taken to address these.

Overall, our inspection found the ACIC was compliant with the requirements of the Act. We identified some exceptions to compliance regarding the record-keeping requirements, including clarity in records on the authority relied on to install a surveillance device and reporting to the Minister. We commend the remedial actions the ACIC has taken to address these issues and those outstanding from previous inspections.

The ACIC was cooperative throughout our inspection and provided access to relevant staff and information. The ACIC demonstrated commitment to compliance and were receptive to our findings and suggestions.

[1] In December 2018, amendments were made to the *Surveillance Devices Act 2004,* however agencies' compliance is assessed against the legislation that was in effect at the time they used the power/s.

Introduction

The Act regulates the use of surveillance devices[2] by law enforcement agencies. 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.[3] It also imposes reporting obligations on law enforcement agencies to ensure appropriate transparency regarding agencies' covert surveillance device activities.

What we do

The Ombudsman performs the independent oversight mechanism provided 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 Minister for Home Affairs) 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. This is why the Ombudsman's oversight role is important in ensuring that these powers are used in accordance with the Act and there is accountability in instances of non-compliance. The Ombudsman's reporting obligations under the Act provides transparency to the Minister and the public on the use of these intrusive covert powers.

How we oversee agencies

The Office has developed a set of inspection methodologies we apply consistently across all agencies. These methodologies are based on legislative requirements and best practice standards, ensuring the integrity of each inspection.

We focus our inspections on areas of high risk, taking into consideration the impact of non-compliance, for example unnecessary privacy intrusions.

---

[2] Under s 6 of 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.

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

We assess compliance based on the records made available at the inspection, discussions with relevant agency teams, observations of agencies' processes through the information they provide and agencies' remedial action in response to any identified issues. For security reasons, we do not inspect records relating to authorities which are still in force.

To ensure agencies understand what we will be assessing, prior to each inspection, we provide them with a broad outline of our criteria. This helps agencies to identify the most accurate sources of information to assist our inspection and overall compliance assessment.

We encourage agencies to be open in disclosing any instances of non-compliance to our Office, including any remedial action it has taken. If required, we can use our coercive powers to obtain any information relevant to our inspection.

At the end of each inspection we provide the agency with our preliminary findings, which enables them to promptly commence any remedial action that may be required. We may also assist agencies by assessing their policies and procedures, communicating 'best practice' to meet compliance and engaging with their staff outside the formal inspection process.

Our criteria

The objective of our inspections is to assess the extent of compliance with the Act by the agency and its law enforcement officers.

When doing so, we use the following criteria:

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

For more information on our inspection criteria and methodology, see **Appendix A.**

How we report to the Minister

To ensure procedural fairness, we give agencies the opportunity to comment on our draft inspection findings. Once we have considered and, where appropriate, incorporated the agencies' response, the inspection results are considered finalised. The findings from these reports are de-sensitised and form the basis of this biannual report to the Minister.

As a result of this consultation, there will typically be some delay between the date we conduct our inspection and the finalisation of the relevant six-monthly report.

The report provides an overview of the compliance assessments we finalised during the reporting period, and discusses agencies' progress in addressing findings from previous inspections as well as details of any new significant or systemic issues.

We may also report on issues other than instances of non-compliance, such as the adequacies of an agency's policies and procedures to ensure compliance with the Act. We may not include administrative issues or instances of non-compliance where the consequences are negligible, for example when a warrant containing errors was not executed.

Australian Criminal Intelligence Commission

We conducted one inspection of the Australian Criminal Intelligence Commission's (ACIC) surveillance device records from 3–6 September 2018. We identified two issues during the inspection, these findings are discussed below.

This inspection assessed the ACIC's records from 1 January to 30 June 2018.

At this inspection we assessed the following warrants and authorisations, which had expired or were revoked during the relevant period:

- 31 of the 63 surveillance device warrants issued to the ACIC
- 12 of the 15 tracking device authorisations given by the ACIC.

We also assessed the following destructions and retentions of protected information during the period:

- 31 of the 61 destructions
- 20 of the 64 retentions.

We would like to acknowledge the ACIC's careful preparation for this inspection. We also appreciate its action to promptly resolve issues that required clarification, and staff's responsiveness to our inspection findings.

Progress made since the previous inspection

At each inspection, we monitor the ACIC's progress in addressing our previous inspection findings. We identified four issues at the previous inspection, two of which were disclosed by the ACIC. These related to records for the period from 1 July to 31 December 2017.

The main issue identified at the previous inspection related to a surveillance device being used on a premises where the person of interest was no longer reasonably believed, or likely to be (due to being arrested), contrary to s 18 of the Act. The device remained installed and collected protected information for an additional four days after the person of interest was arrested before it was retrieved. After our inspection the ACIC advised that, in addition to a person warrant (s 18(1)(c)), the ACIC had been issued a premises warrant (s 18(1)(a)). The premises warrant was the authority the ACIC had relied on to use the device during the additional four days.

At this inspection we reviewed the ACIC's records and were satisfied the ACIC had appropriately amended its records to correctly reflect that the premises warrant was executed. We were also satisfied with the ACIC's action to provide an amended s 49 report to the Minister, and considered it had taken adequate steps to remedy the other three issues identified at the previous inspection.

Inspection findings

We identified two issues at this inspection:

Finding 1 — Unclear on which authority the ACIC acted under to install a surveillance device on a premises

Finding under criterion 1.1: Did the agency have the proper authority for the use and/or retrieval of the device?

What the Act requires

Under s 18(1)(a) of the Act, a surveillance device warrant authorises the use of a surveillance device on specified premises. Subsection 18(2)(a) provides that a premises warrant also authorises the installation, use and maintenance of the device on the specified premises. Subsection 17(1)(b)(vi) of the Act states that the warrant must specify the premises on which use of the surveillance device is authorised.

Subsection 37(1)(c) allows the use of an optical surveillance device without a warrant where use of the device does not involve entry onto premises without permission, such as public premises.

Section 49 of the Act outlines the reporting requirements for each warrant issued to, and authorisation given by an agency. The reporting obligations in the Act are an important transparency and accountability mechanism for an agency's covert surveillance device activities.

What we identified and the ACIC's remedial action

The ACIC was issued a premises warrant for a specified premise (being a particular unit in a complex) listed on the warrant. The records we inspected indicated that an optical surveillance device was installed in the foyer of the unit listed on the warrant. It was not clear on the records whether, in these circumstances, the foyer formed part of the listed premises or if it was considered a common area for the unit complex.

During the inspection, the ACIC clarified that the executing officer obtained verbal permission from the Property Manager of the units to install the surveillance device

in the foyer of the unit. We were unable to locate a written record to confirm this permission.

It was not clear on the records whether, in installing the device, the ACIC had relied on the authority of the warrant or the permission given by the Property Manager, under s 37 of the Act. We note that, in its s 49 report to the Minister, the ACIC advised the premises warrant was executed.

We suggested the ACIC update its records to include a written record of the conversations in which it obtained verbal permission to enter the premises without a warrant. Further, in the event the ACIC did not rely on the premises warrant but, rather, installed the device under s 37 of the Act, we suggested the ACIC provide the Minister with an amended s 49 report as soon as practicable.

Following the inspection, the ACIC confirmed it had updated its records to reflect the events and conversation leading to installation of the surveillance device under s 37. The ACIC also advised it had drafted, and would provide an amended s 49 report for the Minister, clarifying that the premises warrant was not executed.

Finding 2 — Record-keeping requirements under s 40 of the Act

Finding under criterion 1.2: Were surveillance devices used and/or retrieved in accordance with the authority of warrants and authorisations?

What the Act requires

Section 39 of the Act provides for the use of a tracking device without a warrant, defined as a tracking device authorisation (TDA) under s 6 of the Act.

Subsection 39(1) of the Act states that a law enforcement officer may, with written permission from an appropriate authorising officer, use a tracking device without a warrant in the investigation of a relevant offence. Under s 39(7) of the Act, the authorisation must indicate the period the authorisation remains in force, not exceeding 90 days.

Section 40 states the appropriate authorising officer must make a written record as soon as practicable after they have given the TDA. It also sets out what that record must include.

Agency disclosed non-compliance and remedial action

The ACIC disclosed two instances of non-compliance with the TDA requirements under s 39 of the Act. In these instances the authorising officer had not included the TDAs' period of effect in the written permission, contrary to s 39(7) of the Act.
Once ACIC identified this error, these TDAs were revoked.

The relevant s 49 reports to the Minister reflected that these TDAs were authorised and later revoked.

The ACIC also disclosed one instance that a tracking device was installed prior to a written authority. The ACIC identified and quarantined the protected information captured prior to the written authorisation record.

What we identified and the ACIC's remedial action

Following the ACIC's disclosure, we identified three instances that the ACIC did not comply with the record-keeping requirements under s 40 of the Act. In our view, when an authorising officer gives a TDA, even if it is revoked or not executed, the requirement to keep records under s 40 remains.

We suggested that, if it had not already done so, the ACIC update its records of these tracking device authorisations as soon as practicable, to comply with s 40 of the Act.

Following the inspection, the ACIC advised that its records were updated and new procedures implemented to ensure these administrative requirements are met.

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 surveillance 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.

Inspection focus (1): *Were surveillance devices used in accordance with the Act?*		
Relevant Criteria	**Procedural checks**	**Records-based checks**
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. Was 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 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.	