COMMONWEALTH OMBUDSMAN

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

For the period 1 January to 30 June 2019

AUSTRALIAN COMMISSION FOR LAW ENFORCEMENT INTEGRITY
Records from 1 January to 31 December 2018

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

September 2019

COMMONWEALTH OMBUDSMAN

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

For the period 1 January to 30 June 2019

AUSTRALIAN COMMISSION FOR LAW ENFORCEMENT INTEGRITY
Records from 1 January to 31 December 2018

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

September 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 the inspection conducted by the Office of Commonwealth Ombudsman (the Office) at the Australian Commission for Law Enforcement Integrity (ACLEI) finalised during 1 January to 30 June 2019, under s 55 of the *Surveillance Devices Act 2004* (the Act). Overall, our inspection found ACLEI to be compliant with the requirements of the Act. We identified some exceptions to compliance regarding reporting to the Minister and general administrative errors. We commend the remedial action taken by ACLEI to address all issues, including those outstanding from previous inspections.

Our Office also conducted an inspection at the Australian Federal Police (AFP) during this period, but did not finalise the inspection results within this period. Our results from inspecting the AFP will be included in our next six-monthly report to the Minister in March 2020.

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.

In December 2018, the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, amended the Act. Amendments were implemented to strengthen law enforcement agencies' ability to collect information, specifically by establishing a new warrant called a computer access warrant under Part 2, Division 4 of the Act, as well as new emergency authorisations for access to data held in computers under Part 3 of the Act. Neither ACLEI nor the AFP used these new covert powers during the period. We will monitor agencies' use of these powers during future inspections.

The Ombudsman provides independent oversight by conducting inspections under s 55 of the Act 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 review the actions agencies have taken to address these.

Introduction

The Act regulates the use of surveillance devices[1] 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.[2] 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 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 these powers are used in accordance with the Act and, where this does not occur, agencies are held accountable. The Ombudsman's reporting obligations under the Act provide 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 that are applied 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.

---

1 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.

2 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. To maintain the integrity of live investigations, 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.

We encourage agencies to disclose any instances of non-compliance to our Office, including any remedial action taken.

At the end of each inspection we provide the agency with our preliminary findings, which enables staff 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 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.

During 1 January and 30 June 2019, we used 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.**

For future inspections, our inspection criteria will reflect the recent addition of computer access warrants and authorisations to access data held on a computer.

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 our Office's six monthly report to the Minister.

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 Commission for Law Enforcement Integrity

We conducted an inspection of the Australian Commission for Law Enforcement Integrity's (ACLEI) surveillance device records on 13–14 May 2019.

We identified two issues relating to ACLEI's reports to the Minister under s 49 of the Act. Following the inspection, ACLEI advised it had amended and provided the Minister with revised reports.

We appreciate ACLEI's assistance in facilitating the inspection and commend its preparedness, specifically in collating relevant information and documents.

Inspection details

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

- all 11 surveillance device warrants issued to ACLEI
- the one retrieval warrant issued to ACLEI.

We also assessed all five files of protected information retained by ACLEI during the period.

We did not assess any authorisation or destructions of protected information, as ACLEI advised no authorisations ceased to be in force during the period, nor did it destroy any protected information.

This inspection assessed ACLEI's records from 1 January to 31 December 2018.

Progress made since the previous inspections

At each inspection, we monitor ACLEI's progress in addressing previous inspection findings. We identified one issue at the previous inspection in March 2018, which involved two instances of inaccurate reports to the Minister regarding the type of surveillance device used, contrary to s 49(2)(iii) of the Act. We were satisfied with the remedial action taken by ACLEI to address all previous inspection findings.

Inspection findings

Two issues were identified, one of which was partially disclosed by ACLEI:

Finding 1—Disclosed–Retrieval warrant issued twice by an issuing authority and non-compliance with s 49 reporting obligations

Finding under criterion 3.2: *Were reports properly made?*

What the Act requires

Subsection 49(1) of the Act, states a chief officer of each law enforcement agency to whom a warrant is issued, must as soon as practicable after the warrant ceases to be in force, report to the Minister.

Under s 53(1) of the Act, the chief officer of a law enforcement agency must cause a register of warrants to be kept, including for each warrant, the date the warrant was issued or refused (s 53(2)(a)).

What was disclosed

ACLEI disclosed that an application for a retrieval warrant was made to, and issued by a nominated Administrative Appeals Tribunal (AAT) member. After this warrant was issued, the investigator identified that the warrant incorrectly referenced a person, instead of a vehicle (premises), for the retrieval of a surveillance device.

With the intention to rectify the error, the warrant was returned to the nominated AAT member to be amended. The AAT member annotated the original warrant to indicate that it was 'void' and issued a new warrant.

Both the original warrant and the new warrant were issued under the same warrant number, and filed together with an explanation of the circumstances and actions by the nominated AAT member.

What we found and ACLEI's remedial action

There is no provision in the Act to 'void' a warrant once it has been issued, only to revoke it under either ss 20 or 27 of the Act. According to ACLEI's records, the nominated AAT member did not sign a revocation instrument revoking the original retrieval warrant (s 27(1)). Instead, both warrants were issued using the same warrant number.

In these circumstances we consider it would have been better practice for ACLEI to revoke the original retrieval warrant, under s 27(2) of the Act. This would have

avoided ambiguity in technically having two concurrent warrants issued under the same reference number.

In these circumstances we suggested that ACLEI amend the s 49 report to the Minister, to include information about the original warrant. This will ensure transparency in reporting to the Minister on all issued warrants. We also suggest, if ACLEI has not already done so, that ACLEI update its warrants register to reflect the original retrieval warrant, under s 53 of the Act.

Following the inspection, ACLEI advised that the warrant marked 'void' by the issuing authority has been included in the warrant register, and an s 49 report was delivered to the Minister.

Finding 2—Inaccuracies in s 49 reports to the Minister

Finding under criterion 3.2: *Were reports properly made?*

What the Act requires

Section 49 of the Act outlines the reporting requirements for each warrant issued to, and authorisation given by, an agency. This section states 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. This reporting obligation includes non-executed warrants.

What was disclosed and what we found

ACLEI disclosed one instance, and we identified two instances, where warrants were inaccurately reported to the Minister, contrary to the requirements of s 49 of the Act.

ACLEI disclosed one instance where the s 49 report incorrectly stated the date the warrant ceased, as it did not reflect the extension issued on the warrant. ACLEI advised that an amended report had been provided to the Minister.

When assessing the amended report, we identified the following further inaccuracies:

1. The copy of the warrant annexed to the report was a different warrant, contrary to s 49(1)(e)) of the Act.

2. The information provided in the report was inconsistent with information outlined in other records on file, particularly in relation to whose conversations were overheard, recorded, monitored, listened to or observed (see s 49(2)(b)(v)) and the object in or on which a device was installed (see s 49(2)(b)(viii)).

We also identified one instance where the month the surveillance device was used was stated in the report to be September, when all other records indicated that it was used in August (s 49(2)(b)(iv)).

What we suggested and ACLEI's remedial action

While these particular s 49 issues are predominantly administrative in nature, the reporting obligations in the Act are an important transparency and accountability mechanism regarding an agency's covert surveillance device activities. As such, we suggested that an amended report be made to the Minister as soon as practicable in relation to these warrants.

Following the inspection, ACLEI advised that both amended s 49 reports were delivered to the Minister.

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 s 39, and recorded in accordance with s 40 • warrants were revoked in accordance with s 20, and discontinued in accordance with s 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 records which indicate the chief officer or delegate is satisfied 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 Minister 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.	