COMMONWEALTH OMBUDSMAN

Report to the Minister for Home Affairs on agency compliance with the *Surveillance Devices Act 2004* (Cth)

For the period 1 July to 31 December 2021

WESTERN AUSTRALIA POLICE FORCE
Records from 1 July 2020 to 30 June 2021

LAW ENFORCEMENT CONDUCT COMMISSION
Review of procedures

Report by the Acting Commonwealth Ombudsman,
Penny McKay,
under s 61 of the *Surveillance Devices Act 2004* (Cth)

March 2022

COMMONWEALTH OMBUDSMAN

Report to the Minister for Home Affairs on agency compliance with the *Surveillance Devices Act 2004* (Cth)

For the period 1 July to 31 December 2021

WESTERN AUSTRALIA POLICE FORCE
Records from 1 July 2020 to 30 June 2021

LAW ENFORCEMENT CONDUCT COMMISSION
Review of procedures

Report by the Acting Commonwealth Ombudsman,
Penny McKay,
under s 61 of the *Surveillance Devices Act 2004* (Cth)

March 2022

ISSN 2209-7511 - Print
ISSN 2209-752X – Online

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

EXECUTIVE SUMMARY

This report presents the results of the Commonwealth Ombudsman's inspections conducted under the *Surveillance Devices Act 2004* (the Act) between 1 July to 31 December 2021.

During the reporting period we inspected the records of Western Australia Police Force (WA Police) expiring between 1 July 2020 to 30 June 2021.

Table 1: Summary of the key finding of our inspection

Agency	Inspection dates	Summary of the key finding
WA Police	9 to 12 November 2021	Destruction of protected information completed without authority from the chief officer

We were scheduled to inspect the New South Wales Law Enforcement Conduct Commission's (LECC) records, however the LECC did not have any expiring warrants for the records period (1 July 2020 to 30 June 2021). Through mutual agreement with the LECC, the Office conducted a review of the LECC's surveillance devices policies and procedures to assess compliance with the Act, mitigate any future non-compliance, and influence systemic improvements.

In the first half of 2022 we will inspect the records of other agencies' use of powers under the Act. We will include the findings of these inspections in our next report.

Part 1: SCOPE AND METHODOLOGY

Introduction

1.1. The *Surveillance Devices Act 2004* (the Act) restricts the use, communication and publication of information obtained by using surveillance devices and through access to data held in computers.

1.2. The Act imposes requirements on agencies to store and destroy protected information they obtain when using surveillance devices or through computer access activities. The Act restricts the way agencies may use, communicate, or publish such information and requires them to provide reports about these covert activities.

Our oversight role

1.3. Section 55(1) of the Act requires the Commonwealth Ombudsman (the Ombudsman) to inspect the records of a law enforcement agency to determine the extent of compliance with the Act.

1.4. Section 61(1) of the Act requires the Ombudsman to provide to the Minister for Home Affairs reports with the results of each inspection at 6 monthly intervals. These reports provide transparency to the Minister and the public about how agencies use these intrusive powers.

How we oversee agencies

1.5. Our Office uses the same inspection methodology across all agencies. This methodology is based on legislative requirements and best practice standards. Further detail about our inspection criteria and methodology is provided in **Appendix A**.

1.6. To ensure procedural fairness, we give agencies the opportunity to respond to our draft inspection findings. We then remove any operationally sensitive or classified material, and consolidate the significant findings into our report to the Minister.

1.7. We may also report on matters that do not relate to specific instances of non-compliance, such as the adequacy of an agency's policies and procedures to demonstrate compliance with the Act. We generally do not report on administrative issues or instances of non-compliance where the consequences are negligible.

Part 2: WESTERN AUSTRALIA POLICE FORCE

2.1. From 9 to 12 November 2021, we inspected WA Police's surveillance device records.

Inspection details

2.2. We inspected records of warrants that expired between 1 July 2020 and 30 June 2021. We also reviewed surveillance footage and other internal policies and guidance where necessary to determine the extent of compliance with the Act by WA Police.

Type of record	Records made available	Records inspected
TOTAL	**12**	**10 (83%)**

2.3. The available records consisted of 12 surveillance device warrants.

2.4. Following this inspection, we made 2 suggestions for improvement and 1 better practice suggestion to WA Police. We summarise our key finding below.

Progress since our previous inspection

2.5. We last publicly reported inspection results for WA Police in our September 2021 report to the Minister.

2.6. That report included findings in relation to secure storage of protected information, non-compliance with recordkeeping requirements and failure to revoke warrants when no longer required.

2.7. At this inspection we confirmed WA Police took appropriate action to remedy these issues by updating standard operating procedures, improving investigator awareness and implementing templates with example responses and guidance.

Inspection findings

Finding – Non-compliance with destructions provisions

2.8. We identified 4 warrants where protected information was destroyed by WA Police without adhering to s 46(1)(b) of the Act.

2.9. Section s 46(1)(b) of the Act provides that the chief officer must cause to be destroyed any record comprising of protected information in certain circumstances. In practice, for an agency to adhere to s 46(1)(b), the chief officer would issue a written 'destruction order' specifying the protected information to be destroyed prior to its destruction.

2.10. At the inspection we could not verify the location of protected information from a surveillance device for 4 warrants. Following the inspection, WA Police advised that the protected information was destroyed without an express order from the chief officer.

Suggestions for improvement

2.11. We suggested WA Police ensure a destruction order is in place prior to destroying protected information and establish appropriate delegations for destructions. We also suggested, as a matter of better practice, that WA Police improve officer awareness of destruction requirements.

2.12. WA Police accepted this better practice suggestion and advised they developed a Standard Operating Procedure for destructions, which was disseminated to staff.

Finding – Insufficient detail in s 49 reporting

2.13. Section 49 of the Act requires agencies to report to the Minister on each warrant issued or emergency authorisation or tracking device authorisation given. Section 49(2)(b) of the Act sets out information the report must include.

2.14. We suggested WA Police address 2 instances of insufficient detail in the s 49 report to the Minister. At the time of our inspection we were satisfied WA Police had already implemented measures to prevent this issue from reoccurring, namely increasing investigator awareness, amending templates and implementing quality assurance processes.

2.15. We found recent s 49 reports complied with requirements under s 49(2)(b) of the Act and are satisfied that WA Police has taken appropriate remedial action.

Part 3: NSW LAW ENFORCEMENT CONDUCT COMMISSION'S (LECC)

3.1. From 11 to 15 October 2021, our Office reviewed the LECC's surveillance devices policies and procedures against the requirements of the Act.

3.2. The LECC did not have any expiring warrants or authorisations under the Act for the records period (1 July 2020 to 30 June 2021). The Office conducted a review of the LECC's policies and procedures supporting compliance with the Act.

Summary of our review

3.3. The LECC's surveillance device policy and procedures are predominantly used for exercising powers under the NSW *Surveillance Devices Act 2007*. The Office found the LECC's surveillance devices procedures and guidance were not tailored for the use of Commonwealth powers.

3.4. There are significant differences between the NSW and Commonwealth legislation which should be articulated in the LECC's procedures to mitigate risks of future non-compliance. For example, the LECC's policies and procedures for destructions are not specific to requirements under the Act and did not contain information about timeframes or requirements to destroy or retain protected information under s 46(1) of the Act.

3.5. Given the frequency of findings relating to non-compliance with s 49 of the Act at other agencies we oversee, we also provided advice to the LECC on the requirements of s 49(2)(b) of the Act including the detail required in the reports to the Minister of activities under a warrant or authorisation.

3.6. The LECC responded that it would incorporate requirements of the Act into its surveillance devices procedures and would implement our advice regarding s 49 of the Act.

APPENDIX A – INSPECTION CRITERIA

Objective: To determine the extent of compliance with the *Surveillance Devices Act 2004* (the Act) by the agency and its law enforcement officers (s 55).

1. Was appropriate authority in place for surveillance or data access activity?

1.1 Did the agency have the proper authority for using and/or retrieving the device?

Process checks:

- What are the agency's procedures to ensure that surveillance device warrants and retrieval warrants are properly applied for, and are they sufficient?
- What are the agency's procedures to ensure that tracking device authorisations and emergency authorisations are properly issued, and are they sufficient?
- What are the agency's procedures for seeking extensions and variations of warrants, and are they sufficient?
- What are the agency's procedures for revoking surveillance device and retrieval warrants, and are they sufficient?

Records based checks

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 of the Act
- applications for extensions and/or variations to surveillance device warrants were made in accordance with s 19 of the Act
- applications for retrieval warrants were made in accordance with s 22 of the Act
- 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 of the Act
- written records for emergency authorisations were properly issued in accordance with s 31 of the Act
- applications for tracking device authorisations and retrieval of tracking devices were made in accordance with s 39 of the Act
- tracking device authorisations were properly issued in accordance with s 39 of the Act, and recorded in accordance with s 40 of the Act

1.2 Did the agency have proper authority for computer access/data access activities?

Process checks:

- What are the agency's procedures to ensure that computer or data access warrants, authorisations, extensions, and variations are properly applied for, and are they sufficient?
- What are the agency's procedures to ensure that emergency authorisations for computer access activity are properly issued, and are they sufficient?
- What are the agency's procedures for seeking extensions and variations of warrants, and are they sufficient?

Records based checks

We inspect applications, warrants, authorisations, variations, and other agency records, to assess whether:

- applications for computer access warrants were made in accordance with s 27A or s27B if a remote application of the Act
- applications for extensions and / or variations to computer access warrants were made in accordance with s 27F of the Act
- 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 of the Act
- written records for emergency authorisations were properly issued in accordance with s 31

1.3 Were warrants and authorisations properly revoked?

Process checks:

- What are the agency's procedures to ensure that surveillance device warrants are properly revoked, and are they sufficient?
- What are the agency's procedures to ensure that computer access warrants are properly revoked, and are they sufficient?
- What are the agency's procedures for ensuring that use of surveillance devices is discontinued, and are they sufficient?
- What are the agency's procedures for ensuring that computer access/data access activity is discontinued, and are they sufficient?

Records based checks

We inspect agency records, to assess whether:

- surveillance device warrants were revoked in accordance with s 20, and discontinued in accordance with s 21 of the Act
- computer access warrants were revoked in accordance with s 27G, and discontinued in accordance with s 27H of the Act

2. Was surveillance or data activity in accordance with the Act?

2.1 Were surveillance devices used and/or retrieved in accordance with the authority of warrants or in accordance with the provisions of the Act?

Process checks:

- What are the agency's procedures to lawfully use surveillance devices, and are they sufficient?
- What are the agency's procedures for using surveillance devices without a warrant, and are they sufficient?
- Does the agency have an auditable system for maintaining surveillance devices?
- What are the agency's systems and /or records capturing the use of surveillance devices, and are they sufficient?
- What are the agency's procedures for ensuring warrant conditions are adhered to, and are they sufficient?

Records based checks

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 of the Act
- use of surveillance devices under an emergency authorisation was in accordance with s 32 of the Act
- retrieval of surveillance devices or tracking devices was carried out in accordance with ss 26 and 39(11) of the Act
- use of devices without a warrant were in accordance with ss 37 and 38 of the Act
- use of tracking devices under a tracking device authorisation was in accordance with s 39 of the Act
- any extraterritorial surveillance was in accordance with s 42 of the Act

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.

2.2 Were computer access (data access) activities conducted in accordance with the authority of warrants or an authorisation under the Act?

Process checks:

- What are the agency's procedures for ensuring computer access activity is conducted lawfully, and are they sufficient?
- Does the agency have an auditable system for managing computer access or data access activities?
- What are the agency's systems and/or record capturing activities under a computer access warrant, and are they sufficient?
- What are the agency's procedures for ensuring computer access warrant conditions are adhered to, and are they sufficient?

Records based checks

We inspect the records and reports relating to the use of computer access (data access) activities against corresponding authorisations and warrants, to assess whether:

- computer/data access activity under a warrant was in accordance with s 27E of the Act
- concealment of access under a computer access warrant was in accordance with ss 27E(7) to (9) of the Act
- computer/data access activity under an emergency authorisation was in accordance with ss 32 and 27E of the Act.

3. Is protected information properly managed?

3.1 Was protected information properly stored, used, and disclosed?

Process checks:

- What are the agency's procedures for securely storing protected information, and are they sufficient?
- What are the agency's procedures for ensuring the proper use and disclosure of information, and are they sufficient?
- What are the agency's procedures for protecting privacy?

Records based checks

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) of the Act.

3.2 Was protected information retained or destroyed in accordance with the Act?

Process checks:

- What are the agency's procedures for ensuring that protected information is destroyed in accordance with the Act, and are they sufficient?
- What are the agency's procedures for ensuring that protected information is retained in accordance with the Act, and are they sufficient?
- Does the agency regularly review its protected information to ensure compliance with the Act?

Records based checks

We inspect records relating to the review, retention, and destruction of protected information, including records that indicate whether the chief officer or their delegate was satisfied that protected information can be retained or destroyed (s 46 of the Act).

4. Was the agency transparent and were reports properly made?

4.1 Were all records kept in accordance with the Act?

Process Checks:

- What are the agency's record keeping procedures, and are they sufficient?
- Does the agency maintain a general register and is it accurate?

Records based checks

- We inspect records presented to assess whether the agency has met its record-keeping requirements under ss 51 and 52 of the Act.
- We assess information contained in the original records against what is contained in the general register to check whether the agency has met the requirements under s 53 of the Act.

4.2. Were reports properly made?

Process checks:

- What are the agency's procedures for ensuring that it accurately reports to the Minister and the Commonwealth Ombudsman, and are they sufficient?

Records based checks

- We inspect copies of reports to assess whether the agency has met its reporting requirements under ss 49 and 50 of the Act.
- In conducting this assessment, we cross-check the information contained in the reports against the corresponding original records.

4.3 Did the agency notify the Ombudsman of relevant computer access activities in accordance with the Act?

Process checks:

- What are the agency's policies and procedures to ensure it accurately notifies our Office of relevant computer access activity and are they sufficient?

Records based checks

Did the chief officer of the relevant law enforcement agency notify the Ombudsman in relation to the concealment of access activities under a computer access warrant, where those activities took place more than 28 days after the warrant ceased to be in force, in accordance with the Act?

4.4 Does the agency have a culture of compliance?

Process checks:

- Does the agency undertake regular training for officers exercising powers?
- Does the agency provide support and appropriate guidance material for officers exercising powers?
- Was the agency proactive in identifying compliance issues?
- Did the agency disclose compliance issues to the Commonwealth Ombudsman's office?
- Were issues identified at previous inspections addressed?
- Has the agency engaged with the Commonwealth Ombudsman's office as necessary?