COMMONWEALTH OMBUDSMAN

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

Inspections conducted 1 July to 31 December 2022

Law Enforcement Conduct Commission
Records from 1 July 2021 to 30 June 2022

Western Australia Police Force
Records from 1 July 2021 to 30 June 2022

Report by the Commonwealth Ombudsman, Iain Anderson, under s 61 of the *Surveillance Devices Act 2004* (Cth)

March 2023

COMMONWEALTH OMBUDSMAN

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

Inspections conducted 1 July to 31 December 2022

Law Enforcement Conduct Commission
Records from 1 July 2021 to 30 June 2022

Western Australia Police Force
Records from 1 July 2021 to 30 June 2022

Report by the Commonwealth Ombudsman, Iain Anderson, under s 61 of the *Surveillance Devices Act 2004* (Cth)

March 2023

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: media@ombudsman.gov.au

CONTENTS

OUR REPORT – AT A GLANCE 1

EXECUTIVE SUMMARY 2

PART 1: SCOPE AND METHODOLOGY 3

Introduction 3

Our oversight role 3

How we oversee agencies 3

PART 2: LAW ENFORCEMENT CONDUCT COMMISSION 5

Inspection details 5

Progress since our previous inspection 5

Inspection findings 5

PART 3: WESTERN AUSTRALIA POLICE FORCE 9

Inspection details – Surveillance devices records 9

Progress since our previous inspection 9

Inspection findings 9

APPENDIX A – SURVEILLANCE DEVICES INSPECTION CRITERIA 12

OUR REPORT – AT A GLANCE

Key concepts

A **surveillance device warrant** permits law enforcement to use surveillance devices in circumstances including criminal investigations or to locate and safely recover a child to whom recovery orders relate.

There are **four types of surveillance devices**: tracking devices, optical surveillance devices, listening devices and data surveillance devices. Some devices are a combination of two or more of the above devices.

A **computer access warrant** permits law enforcement to collect information from a computer to obtain evidence for a criminal investigation or to locate and safely recover a child to whom recovery orders relate.

Findings

We made **1 formal recommendation** for remedial action.

We made **10 suggestions** and **7 better practice suggestions**.

Our findings related to topics including:

- the overall governance framework for using powers under the *Surveillance Devices Act 2004* (the Act)
- execution of warrants
- privacy considerations
- reporting to the Minister
- record keeping, destruction and storage requirements.

Key messages from this report

- We conducted inspections of the New South Wales Law Enforcement Conduct Commission (LECC) and Western Australia Police Force (WA Police) during the period 1 July to 31 December 2022.
- We found the LECC's governance and compliance framework was not sufficient to support compliance with the Act, as it focused on requirements in state legislation (which differs from the Act).
- We also explored issues demonstrating compliance with the Act when WA Police received technical assistance from a Commonwealth agency to execute its warrants.

EXECUTIVE SUMMARY

This report presents the results of the Office of the Commonwealth Ombudsman's (the Office) inspections conducted under the *Surveillance Devices Act 2004* (the Act) between 1 July and 31 December 2022 (the reporting period).

During the reporting period we inspected the records of the Law Enforcement Conduct Commission of NSW (LECC) and Western Australia Police Force (WA Police).

Table 1 – Summary of key issues identified during each inspection

Agency	Inspection dates	Summary of results of each inspection
LECC	12 to 15 December 2022	We found LECC's governance framework was not fit-for-purpose for its use of Commonwealth surveillance device powers under the Act. We identified action it took under a computer access warrant at a premises was not authorised under the warrant. We identified a lack of privacy considerations in applications for warrants. We also found non-compliance in meeting the reporting requirements to the Minister.
WA Police	13 to 16 September 2022	We identified non-compliance in transferring responsibility for a warrant to a law enforcement officer executing the warrant. We identified issues associated with receiving technical assistance from an external agency to execute WA Police warrants.

Part 1: SCOPE AND METHODOLOGY

Introduction

1.1. The *Surveillance Devices Act 2004* (the Act) sets out the powers of law enforcement agencies (including specified state and territory agencies) with respect to the use of surveillance devices, and access to, and disruption of, data held in computers.

1.2. The Act restricts the use, communication and publication of information obtained by using surveillance devices and through access to data held in computers.

1.3. The Act imposes requirements on agencies to store and destroy protected information obtained by using surveillance devices, through computer access or data disruption activities.

1.4. Agencies using powers under the Act must comply with reporting requirements and are subject to oversight by the Commonwealth Ombudsman (the Ombudsman).

Our oversight role

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

1.6. Section 61(1) of the Act requires the Ombudsman to provide reports to the Minister (the Attorney-General) at 6 monthly intervals with the results of each inspection conducted during the reporting period. These reports provide transparency to the Attorney-General and the public about how agencies use these intrusive powers.

How we oversee agencies

1.7. Our Office's inspection methodology is based on legislative requirements and best practice standards. Further detail about our inspection criteria and methodology is provided at **Appendix A**.

1.8. Using a risk-based approach, we assess an agency's compliance by reviewing a selection of the agency's records, discussions with relevant agency staff, observations of agency policies and processes, and an assessment of remedial action taken in response to issues we had previously identified.

1.9. Our inspections may identify a range of issues from minor administrative errors through to serious non-compliance that affects an individual's rights (notably privacy), the validity of evidence collected, or systemic issues. If an issue is sufficiently serious or systemic, or was previously identified and not resolved, we may make formal recommendations for remedial action. Where an issue of non-compliance is less serious or was not previously identified, we generally make suggestions to the agency to address the non-compliance and to encourage it to identify and implement practical solutions. We may also make better practice suggestions where we consider an agency's existing practice may expose it to compliance risks in the future.

1.10. To ensure procedural fairness, we give agencies the opportunity to respond to our inspection findings. We then consolidate the significant findings into the Ombudsman's 6 monthly report to the Attorney-General.

1.11. This report provides a summary of the most significant findings regarding agencies' compliance with the Act from inspections conducted in the reporting period. 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 do not generally comment in this report on administrative issues or instances of non-compliance where the consequences are low risk.

1.12. We follow up on any remedial action agencies have taken to address our findings at our next inspection.

Part 2: LAW ENFORCEMENT CONDUCT COMMISSION (NSW)

Inspection details

2.1. From 12 to 15 December 2022, we inspected LECC's surveillance device records. We inspected records of warrants that expired between 1 July 2021 and 30 June 2022.

2.2. The available records consisted of 3 surveillance device warrants and 3 computer access warrants.

Table 2 – Summary of records for LECC inspection

	Records made available	Records inspected
TOTAL	**6**	**6 (100%)**

Progress since our previous inspection

2.3. Our previous inspection of LECC's surveillance device records was conducted in October 2021. Inspection results were published in our March 2022 report to the Minister.

2.4. We reported that LECC's surveillance devices procedures and guidance were not tailored for the use of Commonwealth powers. We also provided advice to LECC on the requirements of s 49(2)(b) of the Act, including the detail required in reports to the Minister regarding activities under a warrant or authorisation.

2.5. During our inspection in December 2022, we found that despite updates made since our previous inspection, LECC's procedures and guidance for use of powers under the Commonwealth Act were still not fit-for-purpose. This formed the basis of our primary finding and resulting recommendation.

Inspection findings

2.6. We made 8 findings, resulting in 1 recommendation, 8 suggestions and 3 better practice suggestions.

Finding – No fit-for-purpose governance framework for use of powers under the Surveillance Devices Act 2004

2.7. We found LECC did not have a fit-for-purpose governance framework for using powers under the Commonwealth Act.

2.8. LECC's procedures remained focused on the exercising of powers under the New South Wales *Surveillance Devices Act 2007* and were not sufficiently tailored to the Commonwealth powers. The lack of detail and ease in finding information specific to the Act likely contributed to the non-compliance issues found in the records inspected.

2.9. We recommended LECC establish a fit-for-purpose governance framework for using powers under the Act. This should include standalone procedures and guidance (including to support destruction requirements) and clear roles and responsibilities.

2.10. LECC accepted the basis of this finding and undertook to draft standalone procedures on the use of Commonwealth powers under the Act. However, LECC suggested a formal recommendation based on this finding was not reasonable in the circumstances. LECC referred to the previous inspection's better practice suggestion and noted it had updated its procedures to address shortcomings identified in the 2021 inspection.

Finding – Activities conducted outside the warrant

2.11. We found one instance where action was taken under a computer access warrant at a premises which was not authorised under the warrant. This might suggest action has been unlawfully conducted, and if any material was obtained it may not have been validly collected.

2.12. We suggested LECC seek legal advice about any consequences of the actions taken at premises which were not covered by the warrant.

2.13. LECC accepted our suggestion and will also discuss this type of warrant compliance issue in annual compliance training.

Finding – No privacy considerations outlined in applications

2.14. When determining whether to issue a surveillance device warrant or computer access warrant, the Act requires an eligible Judge or

nominated AAT member to have regard to the extent to which the privacy of any person is likely to be affected.

2.15. We identified 5 records where LECC's applications failed to address the privacy impacts on persons likely to be affected by the warrant.

2.16. Providing information on impacts to a person's privacy can assist eligible judges and AAT members when deciding whether to grant the warrant. It also enhances our Office's ability to assure the Parliament and public that LECC has given due consideration to proportionality and necessity in exercising the powers under the Act.

2.17. We suggested LECC ensure a sufficient assessment and explanation of privacy impacts is included in each application to assist an eligible Judge or nominated AAT member when considering the extent to which the privacy of any person is likely to be affected.

2.18. LECC advised that these were the first warrants issued to the LECC under the Commonwealth Act, and that the privacy elements of its applications were consistent with its practices under NSW surveillance device legislation. LECC advised it has amended its procedures to require the inclusion of a specific privacy section in its warrant applications under the Commonwealth Act, which will also be reviewed by its internal compliance team.

Finding – Inaccuracies and insufficient detail in s 49 reports to the Minister

2.19. Section 49 of the Act requires the chief officer of a law enforcement agency to report to the Minister about each use of warrants, emergency authorisations and tracking device authorisations. The report must be provided to the Minister as soon as practicable after the warrant or authority ceases to be in force. Subsections 49(2)-(3) specify what must be included in the report.

2.20. We identified inaccuracies and insufficient information in s 49 reports to the Minister contrary to the Act. These included:

- incorrectly reporting that a warrant had not been executed, when in fact it had been executed
- inaccurately reporting the number of surveillance devices used
- incorrect references to relevant sections of the Act.

2.21. There were also 3 instances where the s 49 report to the Minister was signed by a compliance officer rather than the chief officer, as required by s 49(1) of the Act.

2.22. We made 2 suggestions and 1 better practice suggestion for LECC to ensure all s 49 reports were correctly notified to the Minister, that future reports are signed by the chief officer or approved delegate, and templates and guidance documents include correct legislative references and guidance to support officers to include more detail.

2.23. LECC accepted our finding and has actioned our suggestions and better practice suggestion.

Finding – Inaccurate information provided in annual report to the Minister

2.24. Section 50 of the Act requires the chief officer of a law enforcement agency to submit a report to the Minister each financial year. Section 50(1) outlines the information that must be provided in the report, which includes the number of warrants issued, and number of emergency authorisations and tracking device authorisations given, in respect of each type of surveillance device.

2.25. We identified that LECC incorrectly overstated the number of tracking device authorisations made by its law enforcement officers in its annual report to the Minister for the year ending 30 June 2022.

2.26. We suggested LECC provide an addendum to the Minister regarding the incorrect information.

2.27. LECC accepted our suggestion and advised it will provide an addendum to next year's annual report to the Minister.

Part 3: WESTERN AUSTRALIA POLICE FORCE

Inspection details – Surveillance devices records

3.1. From 13 to 16 September 2022, we inspected WA Police's surveillance device records. We inspected records of warrants and authorisations that expired between 1 July 2021 and 30 June 2022.

3.2. We inspected 4 of the 7 available records, which were all surveillance device warrants.

Table 3 – Summary of records for WA Police inspection

	Records made available	Records inspected
TOTAL	**7**	**4 (57%)**

Progress since our previous inspection

3.3. We last reported inspection results for WA Police in our March 2022 report to the Minister. That report included findings of non-compliance with the destruction provisions of the Act and insufficient detail in its reporting obligations to the Minister (pursuant to s 49 of the Act).

3.4. WA Police was responsive to the suggestions in our previous report and at this inspection we confirmed that WA Police took appropriate action in relation to our previous findings.

Inspection findings

3.5. We made 3 findings which resulted in 2 suggestions and 4 better practice suggestions.

Finding – Transfer of responsible law enforcement officer for a warrant without written instrument

3.6. A surveillance device warrant must include the name of the law enforcement officer primarily responsible for executing the warrant. Section 6(3) of the Act provides that if the chief officer of a law enforcement agency is satisfied that the law enforcement officer responsible for executing a warrant ceases to have responsibility for

the execution then the chief officer may nominate, in writing, another person as the law enforcement officer primarily responsible for executing the warrant or authorisation.

3.7. We identified one instance where the responsible officer named on the warrant was different to the responsible officer listed on the s 49 report to the Attorney-General. WA Police advised that the responsible officer left the operational area and responsibility for the warrant transferred to another officer. However, there was no written nomination providing for the change of responsible officer. Failing to comply with requirements of the Act may raise questions of lawfulness.

3.8. We suggested that WA Police seek legal advice about the validity of actions taken under the warrant. We also suggested, as a matter of better practice, that WA Police update its guidance material to include the requirements under the Act and to make their staff aware of these requirements.

3.9. WA Police accepted our finding and committed to developing procedures to ensure compliance with s 6(3) of the Act in the future.

Finding – Provision of technical assistance by an external agency and impact on record keeping, destruction and storage requirements

3.10. Three of the warrants inspected involved an external Commonwealth agency providing technical assistance to WA Police to execute the warrant. In these instances, the external agency maintained the complete record of protected information (obtained by the surveillance device) on their systems, with a copy of data provided to WA Police.

3.11. We were not satisfied that WA Police met the requirements of s 46(1)(a) of the Act, which requires the chief officer of a law enforcement agency to ensure that every record or report comprising protected information is kept in a secure place that is not accessible to people who are not entitled to deal with that information.

3.12. WA Police advised that they relied on s 18(3)(g) of the Act to receive this technical assistance. We suggested that WA Police obtain legal advice about the following potential compliance issues:

- whether the external agency's actions went beyond the provision of technical assistance defined in s 18(3)(g) of the Act

- any impact on record keeping, destruction and storage requirements under the Act, including:

    - whether WA Police complied with its obligations under s 46(1)(a) of the Act to ensure that every record comprising protected information is kept secure and is not accessible to people not entitled to deal with the information

    - whether WA Police complied with the use and communication requirements of s 52(1)(e)-(f) of the Act.

3.13. We suggested, as a matter of better practice, that WA Police establish clear policies and procedures outlining the legislative basis under which an external agency may provide technical assistance.

3.14. We also suggested, as a matter of better practice, that WA Police ensure protected information collected under the warrants is destroyed by the external agency (in accordance with s 46 of the Act) once it has been ingested into WA Police's system. Through this process, WA Police should also seek to identify any other protected information being stored by external agencies and ensure this protected information is managed in accordance with s 46 of the Act.

3.15. In response, WA Police advised that it was satisfied that the protected information was stored on a secure device that was not accessible to any person other than the person providing the assistance, and that the information had not been used by any person of the external agency other than the person providing the assistance. Notwithstanding its position, WA Police committed to reviewing its practices for when technical assistance is provided by an external agency, including the collection and storage of data, the provision of data to WA Police, record keeping and destruction requirements.

3.16. WA Police also committed to adopting our better practice suggestion that it ensures protected information collected under the warrants is destroyed by the external agency (in accordance with s 46 of the Act).

APPENDIX A – SURVEILLANCE DEVICES 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 made 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 of the Act.

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 was 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?