COMMONWEALTH OMBUDSMAN

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

For the period 1 January to 30 June 2017

AUSTRALIAN COMMISSION FOR LAW ENFORCEMENT INTEGRITY
Records from 1 July 2015 to 30 June 2016

the former AUSTRALIAN CRIME COMMISSION
Records from 1 July 2015 to 30 June 2016

AUSTRALIAN FEDERAL POLICE
Records from 1 July 2015 to 30 June 2016

NEW SOUTH WALES POLICE FORCE
Records from 1 July 2015 to 30 June 2016

WESTERN AUSTRALIA POLICE
Records from 1 July 2015 to 30 June 2016

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

September 2017

COMMONWEALTH OMBUDSMAN

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

For the period 1 January to 30 June 2017

AUSTRALIAN COMMISSION FOR LAW ENFORCEMENT INTEGRITY
Records from 1 July 2015 to 30 June 2016

the former AUSTRALIAN CRIME COMMISSION
Records from 1 July 2015 to 30 June 2016

AUSTRALIAN FEDERAL POLICE
Records from 1 July 2015 to 30 June 2016

NEW SOUTH WALES POLICE FORCE
Records from 1 July 2015 to 30 June 2016

WESTERN AUSTRALIA POLICE
Records from 1 July 2015 to 30 June 2016

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

September 2017

ISSN 2204-4035

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

INTRODUCTION

The *Surveillance Devices Act 2004* (the Act) regulates the use of surveillance devices[1] by law enforcement agencies. Broadly speaking, the Act allows certain surveillance activities to be conducted under a warrant (issued by an eligible Judge or nominated Administrative Appeals Tribunal member), an internally issued authorisation or without formal authority. The Act imposes requirements for the secure storage and destruction of records, and restricts the use, communication and publication of information obtained through the use of surveillance devices.[2] It also imposes reporting obligations on law enforcement agencies to ensure an appropriate level of transparency.

What we do

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

Why we oversee agencies

The use of surveillance devices is one of the most intrusive covert powers afforded to law enforcement agencies, and part of the Ombudsman's role is to provide the Minister and the public assurance that agencies are using their powers as Parliament intended and, if not, hold the agencies accountable.

How we oversee agencies

We have developed a set of inspection methodologies that we apply consistently across all agencies. These methodologies are based on legislative requirements and best-practice standards in auditing, and ensure the integrity of each inspection.

We focus our inspections on areas of high risk and take into consideration the impact of non-compliance; for example, unnecessary privacy intrusion.

We form our assessments based on the records made available at the inspection, discussions with relevant teams, processes we observe and information staff provide in response to any identified issues. To ensure that agencies are aware of what we will be assessing, we provide them with a

[1] Under the Act, a 'surveillance device' means a data surveillance device, a listening device, an optical surveillance device or a tracking device (or a device that is a combination of any two or more of these devices).

[2] This is collectively referred to as 'Protected Information' and is defined under s 44 of the Act.

broad outline of our criteria prior to each inspection. This assists agencies to identify sources of information to demonstrate compliance. We can rely on coercive powers to obtain any information relevant to the inspection.

We also encourage agencies to be upfront and self-disclose any instances of non-compliance to our Office and inform us of any remedial action the agency has taken.

At the end of each inspection we provide our preliminary findings to the agency to enable the agency to take any immediate remedial action.

We may also assist agencies in ensuring compliance through assessing agencies' policies and procedures, communicating 'best-practices' in compliance, and engaging with agencies outside of the inspection process.

Our criteria

The objective of our inspections is to determine the extent of compliance with the Act by the agency and its law enforcement officers, and we use the following criteria to assess compliance.

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

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

How we report

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

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

We may also discuss issues other than instances of non-compliance, such as the adequacies of an agency's policies and procedures to ensure compliance with the Act. Examples of what we may not include in this report are administrative issues or instances of non-compliance where the consequences are negligible, for example, when actions did not result in unnecessary privacy intrusion.

Relevant agencies

This report includes the results of our inspection of the Australian Commission for Law Enforcement Integrity (ACLEI), the former Australian Crime Commission (ACC)[3], Australian Federal Police (AFP), New South Wales Police Force (NSWPF) and Western Australia Police (WA Police). All these agencies are defined as a 'law enforcement agency' under s 6(1) of the Act.

[3] From 1 July 2016 the ACC and CrimTrac merged to form the Australian Criminal Intelligence Commission. However, as the inspection covered records from when the ACC was still an entity, it will continue to be referred to as such for the purpose of this report.

FINDINGS

The following tables provide an overview of all inspection findings across each agency.

Agency	Australian Commission for Law Enforcement Integrity	Australian Crime Commission	Australian Federal Police
Inspection period[4]	1 July to 31 December 2015	1 July to 31 December 2015	1 July to 31 December 2015
Number of records inspected	ACLEI advised that no warrants or tracking device authorisations expired or were revoked, nor was any protected information retained or destroyed.	37/161 warrants 7/7 tracking device authorisations 12/46 destructions The ACC advised that it did not retain any protected information.	58/298 warrants 6/36 tracking device authorisations 62/184 destructions The AFP advised that it did not retain any protected information.
Criteria	*Inspection findings*		
1. Did the agency have the proper authority for the use and/or retrieval of the device?	No inspection conducted.	Compliant, except in one instance.	Compliant, except in five instances.
2. Were surveillance devices used and/or retrieved in accordance with the authority of warrants and authorisations?	No inspection conducted.	Compliant.	Compliant, except in four self-disclosed instances.
3. Is protected information properly stored, used and disclosed?	No inspection conducted.	Compliant.	Compliant.
4. Was protected information properly destroyed and/or retained?	No inspection conducted.	Compliant, except in 14 instances, five of which were self-disclosed.	Compliant, except in eight instances, two of which were self-disclosed, and one instance where we were unable to determine compliance.
5. Were all records kept in accordance with the Act?	No inspection conducted.	Compliant.	Compliant.
6. Were reports properly made?	No inspection conducted.	Compliant.	Compliant.
7. Was the agency cooperative and frank?	No inspection conducted.	The ACC and the AFP were cooperative and provided access to relevant staff and information during the inspections.	

[4] Inspection period refers to the period during which warrants and authorisations either expired or were revoked.

Agency	Australian Commission for Law Enforcement Integrity	Australian Crime Commission	Australian Federal Police
Inspection period	1 January to 30 June 2016	1 January to 30 June 2016	1 January to 30 June 2016
Number of records inspected	4/4 warrants ACLEI advised that no tracking device authorisations expired or were revoked, nor was any protected information retained or destroyed.	40/111 warrants 10/14 tracking device authorisations 23/30 destructions The ACC advised that it did not retain any protected information.	60/435 warrants 20/23 tracking device authorisations 44/261 destructions 4/73 retentions
Criteria	*Inspection findings*		
1. Did the agency have the proper authority for the use and/or retrieval of the device?	Compliant.	Compliant, with two instances where we were unable to determine compliance.	Compliant, with two instances where we were unable to determine compliance.
2. Were surveillance devices used and/or retrieved in accordance with the authority of warrants and authorisations?	Compliant.	Compliant, with one instance where we were unable to determine compliance.	Compliant, except in six instances, five of which were self-disclosed.
3. Is protected information properly stored, used and disclosed?	Compliant.	Compliant.	Compliant.
4. Was protected information properly destroyed and/or retained?	No destructions or retentions were undertaken during the inspection period.	Compliant.	Not compliant.
5. Were all records kept in accordance with the Act?	Compliant.	Compliant.	Compliant.
6. Were reports properly made?	Compliant.	Compliant.	Compliant.
7. Was the agency cooperative and frank?	ACLEI, the ACC and the AFP were cooperative and provided access to relevant staff and information during the inspections.		

Agency	New South Wales Police Force	Western Australia Police
Inspection period	1 July 2015 to 30 June 2016	1 July 2015 to 30 June 2016
Number of records inspected	4/4 warrants	2/2 warrants
Criteria	*Inspections findings*	
1. Did the agency have the proper authority for the use and/or retrieval of the device?	Compliant, with an administrative issue noted.	Compliant.
2. Were surveillance devices used and/or retrieved in accordance with the authority of warrants and authorisations?	Compliant, except in two instances where we were unable to determine compliance.	Compliant.
3. Is protected information properly stored, used and disclosed?	Compliant.	Compliant.
4. Was protected information properly destroyed and/or retained?	No destructions or retentions were undertaken during the inspection period.	No destructions or retentions were undertaken during the inspection period.
5. Were all records kept in accordance with the Act?	Compliant.	Compliant.
6. Were reports properly made?	Not compliant.	Compliant.
7. Was the agency cooperative and frank?	The NSWPF and WA Police were cooperative and provided access to relevant staff and information during the inspections.	

AUSTRALIAN COMMISSION FOR LAW ENFORCEMENT INTEGRITY

We conducted an inspection of ACLEI on 10 October 2016 for the period 1 January to 30 June 2016. No recommendations or suggestions for improvement were made as a result of the inspection. No inspection was conducted for the period 1 July to 31 December 2015, as ACLEI advised that no surveillance devices warrants or tracking device authorisations expired or were revoked during the period, nor was any protected information retained or destroyed.

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

Findings from previous inspections

We are satisfied that ACLEI has taken appropriate remedial action in relation to the destruction issue identified at the previous inspection.

AUSTRALIAN CRIME COMMISSION

We conducted our first inspection of the ACC from 15 to 18 February 2016 for the period 1 July to 31 December 2015 and our second inspection from 12 to 15 September 2016 for the period 1 January to 30 June 2016. No recommendations were made as a result of either of these inspections, however the ACC self-disclosed and we identified a small number of issues, the most significant of which are discussed below.

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

Findings from previous inspections

Although no recommendations were made as a result of the two previous inspections, a number of issues were identified. We are satisfied that the ACC has taken appropriate remedial action in relation to these issues.

Findings from the first inspection

Finding 1 – Criterion 4

What the Act allows

Under s 46(1)(b) of the Act, as soon as practicable after a record comprising protected information is created, the chief officer must ensure that the record is destroyed, if they are satisfied that the record is no longer required. The chief officer may decide to retain protected information, however, this decision must be recorded. The decision to retain or destroy protected information must be made within five years after its creation. If the chief officer decides to retain protected information, the decision must be made every five years until the protected information is destroyed. Section 46(3) provides an exception to this requirement for protected information that has been received into evidence in legal or disciplinary proceedings.

Therefore, in assessing an agency's compliance with s 46(1)(b), we would expect to see:

- evidence that an agency had obtained appropriate approval to destroy the protected information;
- evidence that the protected information had been destroyed;
- evidence that an agency has conducted regular reviews of protected information to assess if it is still required; and

- if protected information is still required after a period of five years, certification from the chief officer (or delegate) that the protected information may be retained (and certification for every five year period thereafter).

Self-disclosed non-compliance by the ACC

- Four instances where warrants were authorised for destruction, however the authorising officer did not have the delegation under the Act to do so.

- One instance where protected information was destroyed without the proper approval.

What we found

- Three files which contained protected information were retained despite having been authorised for destruction by the chief officer (or delegate). We note that the title of each of these files did not include the reference number of the warrant, which may have caused them to be overlooked for destruction. Subsequent to the inspection, the ACC advised that the protected information has been destroyed.

- One instance where protected information was destroyed without the proper approval.

Response and remedial action taken by the ACC

As a result of these instances, the ACC is undertaking a review of its current destructions program to identify additional search criteria which can be implemented for future destructions rounds. The ACC has amended its processes for storing and destroying protected information and made it consistent with other destruction processes. The ACC has also amended its procedures to include a reminder to staff of their destruction responsibilities under s 46 of the Act.

We also identified some recording and reporting errors under Criteria 5 and 6; despite this, our Office is satisfied the ACC's procedures in relation to these criteria are sufficient to ensure compliance with the Act.

Findings from the second inspection

Finding 1 – Criterion 2

What the Act allows

Under s 18(1)(a) of the Act, a surveillance device warrant may authorise the use of a surveillance device on a specified premises. Section 18(2)(a)(i) further provides that a warrant of this kind authorises the installation, use and maintenance of a surveillance device on the premises specified by the warrant. Section 37(1)(c) of the Act provides for the use of an optical surveillance device, provided that it does not involve entry onto premises without permission.

What we found

We identified one instance where we were unable to determine compliance with the Act regarding the installation, use and retrieval of a surveillance device. The ACC was issued a warrant, authorising the use of surveillance devices on a specified premises. However, the surveillance device was installed and used on an adjoining location outside the specified premises.

In addition, the ACC self-disclosed it had quarantined 10 hours of protected information captured from the use of the surveillance device after the warrant had expired.

There was some ambiguity as to whether a warrant was necessary in this circumstance, which prompted our Office to seek clarification regarding this scenario from the Attorney-General's Department (AGD). In response, the AGD stated that independent legal advice should be sought.

Suggestion and ACC response

In response to our suggestion that the ACC should seek independent legal advice, it advised it had conducted an internal review of the warrant and determined that as the device was an optical surveillance device, that the installation could have arguably attracted powers under s 37(1)(c), as it had permission from the occupier. We understood the ACC's response and advice, however, as we had not sighted records to verify that the occupier had provided permission, we could not confirm compliance with the Act in this instance.

AUSTRALIAN FEDERAL POLICE

We conducted our first inspection of the AFP from 22 to 25 February 2016 for the period 1 July to 31 December 2015 and our second inspection from 5 to 8 September 2016 for the period 1 January to 30 June 2016. No recommendations were made as a result of either of these inspections, however the AFP self-disclosed and we identified a number of issues, the most significant of which are discussed below.

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

Findings from previous inspections

Although no recommendations were made as a result of the two previous inspections, a number of issues were identified. We are satisfied with the remedial action taken by the AFP against all but one issue identified, regarding its non-compliance with s 46 of the Act, relating to the destruction and retention of protected information.

We have reported on this non-compliance over the past three years, and we note that the AFP has taken some remedial action, including disseminating guidance to staff of the relevant legislative requirements. As we identified a further eight instances at our first inspection and 18 instances at our second inspection of non-compliance, the AFP advised of additional remedial action, which is discussed below on page 16 (Finding 5 – Criterion 4). We will continue to monitor the AFP's progress in addressing this issue.

Findings at the first inspection

Finding 1 – Criterion 1

What the Act requires

Under s 40(1)(d) of the Act, an authorising officer must make a written record, as soon as practicable, after giving a tracking device authorisation, and if this relates to a child recovery order it must contain the date the child recovery order was made and the name of the child to whom the child recovery order relates.

What we found

We identified two tracking device authorisations which omitted the date on which the relevant child recovery order had been made and the name of the child to whom the recovery order related.

Response and remedial action taken by the AFP

This issue was identified at our previous inspection and as a result of a suggestion made in our previous report, the AFP advised that it would review its templates to ensure that information required by s 40 of the Act is addressed in future authorisations. The AFP has since advised that the templates are provided by an external Department and it is unable to make amendments. As an alternative, the AFP's compliance team has emailed relevant staff to reiterate the requirement to include all details as per s 40(1)(d). We are satisfied with this remedial action taken by the AFP.

Finding 2 – Criterion 2

What the Act allows

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

Self-disclosed non-compliance and remedial action taken by the AFP

There were two self-disclosed instances where protected information was obtained without proper authority. In both instances, surveillance devices continued to capture protected information after the relevant warrants had expired.

The AFP advised that it ceased monitoring the surveillance devices upon the relevant warrant's expiry and quarantined all protected information from investigators that was captured after its expiration.

Finding 3 – Criterion 2

What the Act allows

Section 42(3)(a) of the Act states that a warrant is taken to permit surveillance in a foreign country, if the surveillance has been agreed to by an appropriate consenting official of the foreign country.

Self-disclosed non-compliance and remedial action taken by the AFP

There were two self-disclosed instances where surveillance devices captured protected information while the target of each surveillance device was located in a foreign country, without consent by an appropriate official.

We note, in one instance the AFP's unsuccessful attempt to deactivate the surveillance device.

In each instance the team responsible for monitoring the surveillance devices was not notified of the international travel but, upon identifying this, the AFP quarantined the protected information captured while the target was located in a foreign country. This was confirmed through secondary checks conducted by our Office and we are satisfied with the AFP's remedial action.

Finding 4 – Criterion 4

What the Act allows

This finding relates to the requirements of s 46 relating to the destruction and retention of protected information (the details of this requirement have been discussed previously on page 8, Finding 1 – Criterion 4).

Self-disclosed non-compliance by the AFP

- Two instances where protected information obtained outside the authority of a warrant was destroyed without the proper approval. We acknowledge that the AFP intended to destroy the unlawfully obtained protected information to ensure compliance, however, the AFP recognised that such destructions still need to be authorised under the Act.

What we found

- Six instances where protected information had been retained for more than five years after it had been created, without the authorisation of the chief officer (or delegate). In each instance, the protected information was ultimately destroyed in accordance with the Act.

- Another instance where protected information had been retained for more than five years after it had been created, without the authorisation of the chief officer (or delegate). In this instance, the protected information was ultimately destroyed; however, it was unclear from available records whether the destruction occurred with proper approval. Therefore, we were unable to determine if the protected information was destroyed in accordance with s 46(1)(b).

We also identified some reporting errors under Criterion 6; despite this, our Office is satisfied the AFP's procedures in relation to this criteria are sufficient to ensure compliance with the Act.

Findings at the second inspection

Finding 1 – Criterion 2

What the Act requires

Under s 39(1) of the Act, a law enforcement officer may, with the written permission of an appropriate authorising officer, use a tracking device without a warrant in the investigation of a relevant offence. Under s 39(6) of the Act, an appropriate authorising officer may also authorise the retrieval, without a warrant, of a tracking device to which the tracking device authorisation relates. The installation, use, maintenance and retrieval of the tracking device is permitted during the time when the authorisation is in force.

What we found

In one instance, a tracking device was not retrieved until after the tracking device authorisation had expired, and the AFP did not obtain a retrieval authorisation to retrieve the tracking device. We confirmed that the tracking device ceased capturing protected information prior to the authorisation's expiry.

Finding 2 – Criterion 2

What the Act requires

Section 18(3)(a) of the Act details that a warrant authorises the retrieval of a surveillance device prior to the expiry of the relevant warrant. Under s 26 of the Act, a law enforcement officer may retrieve a surveillance or tracking device under a retrieval warrant.

What the AFP self-disclosed and what we found

The AFP self-disclosed one instance where a surveillance device was retrieved after the relevant warrant had expired, without a retrieval warrant having been obtained. We confirmed that no protected information was captured by the surveillance device after the warrant expired.

Finding 3 – Criterion 2

What the Act requires

Section 18(2) of the Act details that a warrant authorises the installation of surveillance devices.

Self-disclosed non-compliance and remedial action taken by the AFP

The AFP self-disclosed one instance where surveillance devices were installed prior to a warrant being issued, and therefore without authority. The AFP quarantined the relevant protected information captured prior to the issuing of the warrant. We are satisfied with the AFP's remedial action.

Finding 4 – Criterion 2

What the Act requires

This finding relates to the requirements of s 42(3)(a) regarding surveillance in a foreign country (the details of this requirement have been discussed previously on page 14, Finding 3 – Criterion 2).

What the AFP self-disclosed

There were three self-disclosed instances where surveillance devices captured protected information while the target of each surveillance device was located in a foreign country, with no evidence of consent by an appropriate official.

What we found

In each instance the team responsible for monitoring the surveillance devices was not notified of the international travel but, upon identifying this, the AFP quarantined protected information captured while the target was located in a foreign country.

Finding 5 – Criterion 4

What the Act requires

This finding relates to the requirements of s 46 relating to the destruction and retention of protected information (the details of this requirement have been discussed previously on page 8, Finding 1 – Criterion 4).

What we found

We identified one instance where the written application and tracking device authorisation were destroyed without the approval of the chief officer (or delegate).

There were also 17 instances where protected information had been retained for more than five years after it had been created. This retention was without the authorisation of the chief officer (or delegate) or evidence on file to indicate that the protected information had been given into evidence in legal or disciplinary proceedings. In each instance, the protected information was ultimately destroyed, or further retained, in accordance with the Act.

Response and remedial action taken by the AFP

In relation to the first instance above, the AFP indicated that the issue would be included in future training packages for investigators. In addition, the AFP advised that the current retention process will be reviewed to assist in reducing the number of instances of non-compliance.

We also identified some reporting errors under Criterion 6; despite this, our Office is satisfied the AFP's procedures in relation to this criteria are sufficient to ensure compliance with the Act.

NEW SOUTH WALES POLICE FORCE

We conducted our inspection of the NSWPF on 24 November 2016 for the period 1 July 2015 to 30 June 2016. Although no recommendations were made as a result of this inspection, we identified two issues, which are discussed below.

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

Findings from previous inspections

We are satisfied that the NSWPF has taken appropriate remedial action in relation to the issues identified at the previous inspections.

Findings at this inspection

Finding 1 – Criterion 2

What the Act requires

Under s 18(1)(a) of the Act, a surveillance device warrant may authorise the use of a surveillance device on a specified premises. Section 18(2)(a)(i) further provides that a warrant of this kind authorises the installation, use and maintenance of a surveillance device on the premises specified by the warrant.

What we found

In one instance, we were unable to determine whether a surveillance device was installed on the premises specified on the warrant. Additionally, due to discrepancies in the NSWPF's records, we were unable to determine when two surveillance devices were installed.

Response by NSWPF

Subsequent to the inspection, the NSWPF advised our Office that the surveillance devices were installed in accordance with the warrant. We will review this advice at the next inspection to determine compliance.

Finding 2 – Criterion 6

What the Act requires

Section 49 of the Act sets out the reporting requirements for each warrant issued to the NSWPF. In accordance with s 49, the chief officer must, as soon as practicable after the warrant ceases to be in force, make a report to the Minister and provide copies of the relevant warrants and other specified documents. The Act does not define 'as soon as practicable', however, for the purposes of our inspection we consider that a period of up to three months would satisfy this requirement and beyond this we would expect to be provided reasons for why it was not practicable. These reporting obligations are an important transparency mechanism in the Act.

What we found

For all four warrants the NSWPF had not complied with s 49 of the Act. We identified that the NSWPF had not submitted any reports to the Minister under these provisions, despite the warrants ceasing to be in force between nine months and three years prior to the inspection. As there appeared to be no reason for this, we suggested that the NSWPF provide all of these reports and copies of the warrants to the Minister as a matter of urgency.

Additionally, at the time of the inspection, as the NSWPF had not yet formalised its current procedures in relation to s 49, we were unable to assess if they are sufficient to achieve compliance with the Act.

Response by NSWPF

To achieve future compliance, the NSWPF advised that it has developed a report template and drafted instructions for its officers responsible for executing surveillance device warrants, which address the requirements of s 49. The NSWPF also advised that it will provide relevant training to its officers. We will assess the effectiveness of these measures at future inspections.

WESTERN AUSTRALIA POLICE

We conducted an inspection of WA Police on 7 and 8 November 2016 for the period 1 July 2015 to 30 June 2016. No recommendations or suggestions for improvement were made as a result of the inspection.

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

Findings from previous inspections

During the previous inspection, we identified that the WA Police did not have formal processes to address retaining and destroying protected information in accordance with the Act. At this inspection we were satisfied with the WA Police's remedial action, which included the implementation of standard operating procedures to address these requirements.

APPENDIX A – INSPECTION CRITERIA AND METHODOLOGY

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

2. Were surveillance devices used and/or retrieved in accordance with the authority of warrants and authorisations?	We check that the agency has policies and procedures to ensure that: – 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: • surveillance devices were used in accordance with the relevant warrant (s 18) • surveillance devices were used in accordance with the relevant emergency authorisation (ss 18 and 32) • retrieval of surveillance devices or tracking devices was carried out lawfully (ss 26 and 39(11)) • tracking devices were used in accordance with the relevant tracking device authorisation (s 39) • extra-territorial surveillance was carried out lawfully (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 to capture information from surveillance devices. We may also rely on what we understand of an agency's processes and procedures in determining the veracity of such records, and take into consideration whether the records were made contemporaneously.

Inspection focus (2): *Is protected information properly managed?*		
Relevant Criteria	**Procedural checks**	**Records-based checks**
3. Is protected information properly stored, used and disclosed?	We check that the agency has policies and procedures to ensure that: – 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 that the agency has used and/or communicated protected information for a purpose other than one outlined in s 45(4).
4. Was protected information properly destroyed and/or retained?	We check that the agency has policies and procedures to ensure that: – 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 that the agency has policies and procedures to ensure that: – 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 that the agency has policies and procedures to ensure that 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.	