COMMONWEALTH OMBUDSMAN

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

For the period 1 January to 30 June 2016

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

AUSTRALIAN CRIME COMMISSION
Records from 1 January to 30 June 2015

AUSTRALIAN FEDERAL POLICE
Records from 1 January to 30 June 2015

CRIME AND CORRUPTION COMMISSION
Records from 1 July 2014 to 30 June 2015

NEW SOUTH WALES POLICE FORCE
Records from 1 July 2014 to 30 June 2015

WESTERN AUSTRALIA POLICE
Records from 1 July 2014 to 30 June 2015

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

September 2016

COMMONWEALTH OMBUDSMAN

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

For the period 1 January to 30 June 2016

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

AUSTRALIAN CRIME COMMISSION
Records from 1 January to 30 June 2015

AUSTRALIAN FEDERAL POLICE
Records from 1 January to 30 June 2015

CRIME AND CORRUPTION COMMISSION
Records from 1 July 2014 to 30 June 2015

NEW SOUTH WALES POLICE FORCE
Records from 1 July 2014 to 30 June 2015

WESTERN AUSTRALIA POLICE
Records from 1 July 2014 to 30 June 2015

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

September 2016

ISSN 2204-4027

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 (AAT) 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. This report sets out the results of our inspections finalised between 1 January and 30 June 2016.

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 the agency 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), Australian Crime Commission (ACC)[3], Australian Federal Police (AFP), Crime and Corruption Commission (CCC), 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 ACC was still an entity at the time of our inspection, 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 January to 30 June 2015	1 January to 30 June 2015	1 January to 30 June 2015
Number of records inspected	2/2 warrants 1/1 destruction	38/121 warrants 5/13 tracking device authorisations 20/20 destructions	60/308 warrants 13/27 tracking device authorisations 58/152 destructions 18/25 retentions
Criteria	*Inspection findings*		
1. Did the agency have the proper authority for the use and/or retrieval of the device?	Compliant.	Compliant, with an administrative issue noted.	Compliant, except in 18 instances.
2. Were surveillance devices used and/or retrieved in accordance with the authority of warrants and authorisations?	Compliant.	Compliant, with two exceptions.	Compliant, except in four instances.
3. Is protected information properly stored, used and disclosed?	Compliant.	Compliant.	Compliant.
4. Was protected information properly destroyed and/or retained?	Compliant. One legal issue discussed.	Compliant, except in one instance.	Compliant, except in 12 instances. Unable to determine compliance in nine instances.
5. Were all records kept in accordance with the Act?	Compliant.	Compliant, except in one instance. Findings discussed.	Compliant, except in three instances.
6. Were reports properly made?	Compliant.	Compliant, except in four instances.	Compliant, except in one instance.
7. Was the agency cooperative and frank?	Compliant. ACLEI, 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	Crime and Corruption Commission	New South Wales Police Force	Western Australia Police
Inspection period	1 July 2014 to 30 June 2015	1 July 2014 to 30 June 2015	1 July 2014 to 30 June 2015
Number of records inspected	2/2 warrants	14/14 retentions	1/1 warrant
Criteria	*Inspection findings*		
1. Did the agency have the proper authority for the use and/or retrieval of the device?	Compliant, except in four instances.	No warrants or tracking device authorisations were issued during the inspection period.	Compliant.
2. Were surveillance devices used and/or retrieved in accordance with the authority of warrants and authorisations?	Compliant.	No warrants or tracking device authorisations were issued during the inspection period.	Compliant.
3. Is protected information properly stored, used and disclosed?	Compliant.	Compliant. Nothing to indicate otherwise.	Compliant.
4. Was protected information properly destroyed and/or retained?	No destructions or retentions were undertaken during the inspection period. However, one issue is discussed.	Not compliant with s 46(1)(b).	No destructions or retentions were undertaken during the inspection period.
5. Were all records kept in accordance with the Act?	Compliant.	No warrants or tracking device authorisations were issued during the inspection period.	Compliant.
6. Were reports properly made?	Compliant, except in two instances.	No warrants or tracking device authorisations were issued during the inspection period.	Compliant, except in one instance.
7. Was the agency cooperative and frank?	Compliant. The CCC, 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 our inspection of ACLEI on 27 and 28 October 2015. Although no recommendations were made as a result of the inspection, we identified one issue regarding the destruction of protected information, which is discussed below.

We would also 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 issues identified at previous inspections.

Findings at this inspection

Finding 1 – Criterion 4

What the Act requires
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.

What we found
ACLEI conducted one destruction during the inspection period and we are satisfied that this was done in accordance with the Act.

However, ACLEI advised that protected information was transferred from a device and then stored electronically. ACLEI was unsure whether the transfer (i.e. the removal of information from the device) could be classified as a destruction. If it was, it would need to be done in accordance with s 46 of the Act. We suggested that ACLEI seek legal advice to clarify this.

Further information provided by ACLEI
Since the inspection, ACLEI received legal advice and advised that this transfer has been classified as a destruction.

Suggested practice
We suggested that ACLEI update its policies and procedures to reflect the legal advice in relation to destructions.

AUSTRALIAN CRIME COMMISSION

We conducted our inspection of the ACC from 6 to 8 October 2015. Although three instances of non-compliance were self-disclosed and a further five issues identified, we are satisfied that the ACC has taken adequate remedial action and has sufficient procedures in place to ensure ongoing compliance with the Act.

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

Findings from previous inspections

No recommendations were made and no issues requiring further remedial action were identified at the previous inspection.

Findings at this inspection

Finding 1 – Criterion 2

What the Act allows
Section 18 of the Act states what a surveillance device warrant may authorise. Section 18(3) states that a surveillance device warrant authorises the installation, use, maintenance and retrieval of a surveillance device. Therefore, all activity regarding the use, maintenance and retrieval of a surveillance device should occur in accordance with the authority of the warrant.

Self-disclosed non-compliance
The ACC self-disclosed one instance where a surveillance device was installed under a valid warrant but was retrieved after the warrant had expired. Additionally, there was a second instance where a tracking device was retrieved after the warrant expired, which transmitted protected information onto the ACC's systems until a retrieval warrant was issued nine days later.

Response and remedial action taken by the ACC
In our view, the ACC's systems for monitoring use of devices are sound, however the ACC has advised it has strengthened its 'warrant cessation processes' by providing tailored review sessions and implementing system-automated notices for expiry dates. The ACC and our office expect these changes will reduce the likelihood of future non-compliance with s 18.

Finding 2 – Criterion 4

What the Act requires
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 certified. 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 re-visited every five years until the protected information is destroyed.

Therefore, in assessing an agency's compliance with s 46(1)(b), we would expect to see 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
The ACC self-disclosed one instance where protected information was kept for a period longer than five years without the chief officer certifying that it could be retained.

The protected information was approved for destruction but no further action took place. This was subsequently identified through the ACC's quality assurance checks.

Remedial action taken by the ACC
Upon identification, the protected information was destroyed.

We are satisfied that the ACC has adequate processes and checks in place to achieve compliance with the Act's destruction requirements.

We also identified some recording and reporting errors under criterion 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.

AUSTRALIAN FEDERAL POLICE

We conducted our inspection of the AFP from 29 September to 2 October 2015. No recommendations were made as a result of the inspection, although the AFP self-disclosed nine instances of non-compliance and several further issues were identified during the inspection. These findings resulted in several suggestions to the AFP to amend its processes, policies and procedures to ensure ongoing compliance with the Act.

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

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 AFP has taken appropriate remedial action in relation to these issues.

Findings at this inspection

Finding 1 – Criterion 1

What the Act requires
Under s 40(1) of the Act, an authorising officer must make a written record of any tracking device authorisation given. Section 40(1) specifies the information which must be included in the authorisation.

What we found
During the inspection, we identified two tracking device authorisations that omitted the date on which the relevant child recovery order had been made, contrary to s 40(1)(d).

Suggested practice and AFP response
As no deficiencies were noted in relation to any other tracking device authorisations, this may be due to an omission in the template used for child recovery orders. We suggested that the AFP may wish to review its template to ensure that the information required by s 40 is addressed in future authorisations.

Remedial action taken by the AFP
The AFP has since advised that it will review its template to ensure future compliance with the Act.

Finding 2 – Criterion 1

What the Act allows
Under s 19(1) of the Act, a law enforcement officer to whom a surveillance device warrant has been issued (or another person on his or her behalf) may apply for an extension or a variation to the warrant.

Self-disclosed non-compliance and what we found
The AFP self-disclosed four instances where warrant extensions had been applied for by someone other than the original applicant. During the inspection, we identified a further 12 instances where this had occurred.

In each case, the application coversheet and the affidavit did not indicate that the application was being made on behalf of the original law enforcement officer.

However, we note that in eight of these instances (including those which were self-disclosed) there were handwritten annotations on file which indicated that applications had, in fact, been made on behalf of the original applicant. This may indicate that a recording issue is occurring at the time of the application.

Response and remedial action taken by the AFP
The AFP has since revised its application template and procedures for surveillance device warrants and will make these documents available at the next inspection.

Finding 3 – 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 specified premises. Section 18(2)(a)(i) further provides that a warrant of this kind will authorise the installation, use and maintenance of a surveillance device on the premises specified by the warrant.

Self-disclosed non-compliance
Under one warrant issued under s 18(1)(a), the AFP had installed surveillance devices on portable objects located within the specified premises. Whilst the installations were lawful, this practice increases the risk that surveillance devices will be used outside the specified premises, and outside the authority of the warrant.

The AFP self-disclosed that in this instance, the installation resulted in protected information being collected outside of the premises specified on the warrant. The AFP advised that, as a concurrent warrant for that portable object was not in place, the product was quarantined from investigators. We were able to confirm this advice by checking the systems that investigators access.

The AFP subsequently provided us with additional information as to how the AFP can mitigate the risk of non-compliance in these instances. We encourage the AFP to ensure that such controls are in place before installing surveillance devices on portable objects.

Response and remedial action taken by the AFP
The AFP has advised that it is in the process of updating its procedures, National Guideline and Aide Memoire for surveillance devices to ensure future compliance with the Act.

Finding 4 – Criterion 2

What the Act allows
Section 18 of the Act states what a surveillance device warrant may authorise. Section 18(3) states that a surveillance device warrant authorises the retrieval of a surveillance device. Therefore, all activity regarding the retrieval of a surveillance device should occur in accordance with the authority of the warrant.

Self-disclosed non-compliance
The AFP self-disclosed one instance where, following the expiry of the relevant warrant, it had failed to retrieve or disable a tracking device still installed on a target vehicle.

Response and remedial action taken by the AFP
The AFP advised that, due to technical issues experienced with the device, it had assumed that the device was no longer functioning and as a result there was no need to retrieve or disable it. After identifying that the device was still functioning, the AFP obtained a retrieval warrant and successfully retrieved the device.

The AFP advised that no protected information was captured following the expiry of the warrant as the device had not been 'activated' during this time.

Finding 5 – Criterion 2

What the Act allows
As stated under Finding 4, a surveillance device warrant authorises the retrieval of deployed devices. If the surveillance device warrant has expired, s 22 of the Act allows a law enforcement officer (or another person on his or her behalf) to apply to an eligible Judge or nominated AAT member for the issue of a retrieval warrant for this purpose. Section 26 of the Act states what a retrieval warrant authorises.

Self-disclosed non-compliance
The AFP self-disclosed one instance where a surveillance device was retrieved outside the authority of a warrant.

The relevant surveillance device warrant expired on 1 April 2015, and the device was retrieved on 2 April 2015 in the absence of a retrieval warrant. In this case, the installation and retrieval of the device had been carried out by a state law enforcement agency on behalf of the AFP, in accordance with their own standard operating procedures.

Response and remedial action taken by the AFP
The AFP advised that, as a result, a new procedure was initiated whereby state law enforcement partners are reminded when warrants are due to expire to ensure that all devices are retrieved or deactivated prior to the expiry date.

We note that at the time of the inspection, the AFP was waiting on confirmation that no protected information had been captured by the device following the expiry of the warrant. The AFP has since advised that no protected information was captured, and we will confirm this at our next inspection.

Finding 6 – Criterion 2

What the Act allows
Section 25(1)(b)(iii) of the Act provides that a retrieval warrant must specify the kind of surveillance device authorised to be retrieved. Under s 26(1)(a), a warrant of this kind authorises the retrieval of the surveillance device specified in the warrant.

Self-disclosed non-compliance
The AFP self-disclosed one instance where a device had been retrieved which was not specified in the relevant retrieval warrant. This omission

meant that the subsequent retrieval of the device fell outside the authority of the warrant.

Response and remedial action taken by the AFP
The AFP advised that relevant AFP staff have been reminded to check the details of devices which are still located on specified premises, and ensure that this is accurately reflected in the retrieval warrant.

Finding 7 – Criterion 4

What the Act requires
This finding relates to the requirements of s 46 of the Act relating to the destruction of protected information (the details of this requirement have been discussed previously on page 8, Finding 2 – Criterion 4).

What we found
During the inspection, we identified 12 instances where protected information had been retained for more than five years without the authorisation of the chief officer (or delegate).

There were also two instances where we were unable to determine whether protected information had been retained in accordance with s 46 and seven instances where we were unable to determine whether it had been destroyed in accordance with s 46.

Response and remedial action taken by the AFP
In each of the 12 instances where protected information was retained for longer than five years without authorisation, the AFP advised that all have now been authorised to be retained or destroyed in accordance with the Act. However, this occurred two to five months outside of the legislated five year period.

Subsequent to our inspection, the AFP advised that the nine instances where we were unable to determine compliance, have since been actioned in accordance with the Act.

The APF will make all necessary documents available for review at our next inspection.

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

CRIME AND CORRUPTION COMMISSION

We conducted our inspection of the CCC from 27 to 29 July 2015. No recommendations were made as a result of the inspection, although six instances of non-compliance were identified.

We would also like to acknowledge the CCC's cooperation during the inspection.

Findings from previous inspections

No recommendations were made and no issues requiring further remedial action were identified at the previous inspection.

Improvements

At our previous inspection we noted the CCC's advice that it was in the process of developing guidance documents regarding the issuance of warrants and management of protected information.

At this inspection the CCC advised that the guidance documents had been submitted for approval to the Acting Chairperson in June 2015, but had not yet been approved.

Following the inspection, we were provided with a copy of this draft guidance which we commented on to remove potential gaps in the CCC's destruction process. Subsequent to the inspection, the CCC advised that the draft guidance had been finalised and uploaded on the agency's intranet page in August 2015.

Findings at this inspection

Finding 1 – Criterion 1

What the Act allows
Section 19 of the Act sets out the requirements for the extension or variation of a surveillance device warrant. Section 19(1) provides for the original applicant (or another person on their behalf) to apply for a variation or extension to the warrant.

What we found
During the inspection we identified four instances of non-compliance with s 19(1) of the Act, as the applications for extensions and variations were not made by the original law enforcement officer or another person on their behalf.

In these instances we would expect the variation or extension being made by a person on behalf of the original law enforcement officer to be explicitly recorded in the affidavit supporting the application to the nominated AAT member or eligible Judge.

Response received from CCC
The CCC has indicated that future extension and variation records will be more explicit relating to the applicant.

We also identified some reporting errors under criterion 6, despite this, our office is satisfied the CCC's procedures in relation to this criterion are sufficient to ensure compliance with the Act.

NEW SOUTH WALES POLICE FORCE

We conducted our inspection of the NSWPF on 21 December 2015. Although no recommendations were made as a result of this inspection, we identified 14 warrants which were non-compliant with s 46(1)(b). Subsequent to the inspection, the NSWPF advised that it has taken, what we believe are, appropriate remedial actions to address these issues.

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

Findings from previous inspections

No recommendations were made and no issues requiring further remedial action were identified at our last inspection in 2013.

Findings at this inspection

Finding 1 – Criterion 4

What the Act requires
This finding relates to the requirements of s 46 of the Act relating to the destruction of protected information (the details of this requirement have been discussed previously on page 8, Finding 2 – Criterion 4).

What we found
In response to a recommendation we made in March 2012, the NSWPF implemented a framework for regular reviews of protected information obtained under every warrant and authorisation. As reflected in the agency's standard operating procedures, all warrants that have resulted in protected information being obtained are to be reviewed at least once in every 12 month period, and a decision is to be made as to whether the protected information is to be retained or destroyed.

In addition to the annual reviews, the NSWPF have also implemented a framework for five yearly reviews in relation to protected information obtained under each warrant and authorisation.

However, this procedure falls short of the legislative requirements as it appears that no follow up action is conducted after the reviews. As identified at this inspection, this led to 12 instances where protected information which had been marked as suitable for destruction had not been destroyed.

Furthermore, we identified that protected information obtained under the 14 warrants inspected had been retained for a period longer than five years, without certification from the chief officer (or delegate).

Response and remedial action taken by the NSWPF
Subsequent to the inspection, the NSWPF advised that certificates for retention in relation to these records could not be located, but have now been prepared and will be forwarded to the respective delegate for their consideration.

The NSWPF have further advised that it will conduct a formal review of each warrant identified in this report and will conduct an assessment of its framework and procedures more broadly to ensure future compliance with the Act.

Suggested practice
We suggest that the NSWPF add additional controls and/or oversight to the framework to ensure that certificates of retention are used, and any follow up action required after the reviews takes place.

WESTERN AUSTRALIA POLICE

We conducted our inspection of the WA Police on 15 October 2015. As a result of our inspection we are satisfied that the WA Police is using these covert powers as Parliament intended. We are satisfied that the one instance of non-compliance has been corrected through remedial action.

We would also like to acknowledge the WA Police's cooperation during the inspection and for being forthcoming in providing detailed contemporaneous records that assisted our office in forming our compliance assessment.

Findings from previous inspections

No recommendations were made and no issues requiring further remedial action were identified at the previous inspection.

Improvements

At this inspection we were able to verify the implementation of a best-practice suggestion we made at the previous inspection and commend the WA Police for its responsiveness.

Findings at this inspection

We noted one reporting error under s 49 of the Act. Despite this, our office is satisfied the WA Police's procedures in relation to these criteria are sufficient to ensure compliance with the Act.

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 AAT 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; the agency's overall attitude towards compliance.	