COMMONWEALTH OMBUDSMAN

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

For the period 1 July to 31 December 2019

AUSTRALIAN COMMISSION FOR LAW ENFORCEMENT INTEGRITY
Records from 1 January 2019 to 30 June 2019

AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION
Records from 1 July 2018 to 30 June 2019

AUSTRALIAN FEDERAL POLICE
Records from 1 January 2018 to 30 June 2019

NEW SOUTH WALES POLICE FORCE
Records from 1 July 2017 to 30 June 2019

SOUTH AUSTRALIA POLICE
Records from 1 July 2017 to 30 June 2019

VICTORIA POLICE
Records from 1 July 2017 to 30 June 2019

Report by the Commonwealth Ombudsman,
Michael Manthorpe PSM,
under s 61 of the *Surveillance Devices Act 2004* (Cth)

March 2020

COMMONWEALTH OMBUDSMAN

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

For the period 1 July to 31 December 2019

AUSTRALIAN COMMISSION FOR LAW ENFORCEMENT INTEGRITY
Records from 1 January 2019 to 30 June 2019

AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION
Records from 1 July 2018 to 30 June 2019

AUSTRALIAN FEDERAL POLICE
Records from 1 January 2018 to 30 June 2019

NEW SOUTH WALES POLICE FORCE
Records from 1 July 2017 to 30 June 2019

SOUTH AUSTRALIA POLICE
Records from 1 July 2017 to 30 June 2019

VICTORIA POLICE
Records from 1 July 2017 to 30 June 2019

Report by the Commonwealth Ombudsman,
Michael Manthorpe PSM,
under s 61 of the *Surveillance Devices Act 2004* (Cth)

March 2020

ISSN 2209-752X (Online)
ISSN 2209-7511 (Print)

Contact us
Enquiries regarding the licence and any use of this report are welcome at:

Commonwealth Ombudsman
GPO Box 442
Canberra ACT 2601
Tel: 1300 362 072
Email: ombudsman@ombudsman.gov.au

Contents

Overview

This report presents the results of inspections conducted by the Office of the Commonwealth Ombudsman (the Office) under the *Surveillance Devices Act 2004* (Cth) (the Act) during the period from 1 July to 31 December 2019 (the inspection period). We conducted inspections at the Australian Commission for Law Enforcement Integrity (ACLEI), Australian Criminal Intelligence Commission (ACIC), Australian Federal Police (AFP), New South Wales Police Force, South Australia Police and Victoria Police.

Under the Act, specified law enforcement agencies can covertly use surveillance devices when investigating certain offences. This power is given to Commonwealth agencies for the purposes of combating crime and protecting the community. The Act also allows specified State and Territory law enforcement agencies to use surveillance devices to investigate certain Commonwealth offences and enforce Family Court recovery orders.

The Ombudsman provides independent oversight by regularly inspecting the records of agencies that have exercised Commonwealth surveillance device powers. At these inspections, we assess whether the agency was compliant with the Act during the inspection period and had processes in place to support compliance. We also consider the agency's transparency and accountability, and encourage it to disclose systemic problems or instances of non-compliance to our Office. If we identified problems at an agency at a previous inspection, we review any actions it has taken to address these and monitor agency progress.

The most significant issues identified during the inspection period related to using and retrieving surveillance devices without meeting the Act's requirements and/or obtaining the proper authority. We also identified a number of reporting errors and information management issues. Nevertheless, we found agencies were generally responsive to our findings, and implemented appropriate remedial action. We were also pleased that agencies proactively disclosed instances of non-compliance to us, either when they arose or at the time of our inspection.

In December 2018 the Act was amended by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* to allow agencies to collect information using a new 'computer access warrant'.[1] During the periods relevant to our inspection, the ACIC was issued with one computer access warrant and the AFP with two. Given the very low usage, we were able to examine all three warrants along with the AFP's and the ACIC's procedures to inform our understanding of how they are using the new powers. We anticipate that agencies will use the powers in much greater numbers going forward, and we are considering how best to perform and resource our inspections of the associated records.

[1] Part 2, Division 4 – Computer Access Warrants

Noting that we only inspected a small number of warrants at each agency, we did not identify any compliance issues arising from the ACIC's and AFP's initial use of these powers.

Introduction

The Act regulates the use of surveillance devices by law enforcement agencies. Under s 6 of the Act, a 'surveillance device' means a data surveillance device, a listening device, an optical surveillance device or a tracking device—or a device that is a combination of any two or more of these devices.

The Act allows law enforcement agencies to covertly conduct certain surveillance activities under a warrant issued by an eligible judge or nominated Administrative Appeals Tribunal (AAT) member, an internally issued authorisation, or, in limited circumstances, without formal authority.[2] The Act imposes requirements for agencies to securely store and destroy information obtained by using surveillance devices. These types of information and records are collectively referred to as 'protected information'.[3]

The Act also restricts using, communicating, and publishing such information; and it imposes reporting obligations on law enforcement agencies to ensure appropriate transparency regarding agencies' covert surveillance device activities.

In December 2018 the Act was amended[4] to enhance law enforcement agencies' ability to collect information, by establishing a new warrant called a computer access warrant under Part 2, Division 4 of the Act, as well as new emergency authorisations for access to data held in computers under Part 3 of the Act.

What we do

The Ombudsman performs the independent oversight mechanism set out in the Act. The Ombudsman is required to inspect the records of each law enforcement agency to determine the extent of its compliance with the Act and report the results to the relevant Minister every six months.

Why we oversee agencies

The covert use of surveillance devices by law enforcement agencies is highly intrusive. This is why the Ombudsman's oversight role is important; we ensure these powers are used in accordance with the Act and, where this does not occur, hold agencies accountable. The Ombudsman's reporting obligations under the Act provide transparency to the Minister and the public on the use of these intrusive powers.

---

2 Part 4 of the Act provides the circumstances in which certain surveillance devices may be used without a warrant, for example, the use of an optical surveillance device where that use does not involve entry onto premises without permission.

3 Section 44 of the Act.

4 Schedule 2, *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*.

How we oversee agencies

The Office has developed a set of inspection methodologies that are applied consistently across all agencies. These methodologies are based on legislative requirements and best practice standards, ensuring the integrity of each inspection. We focus our inspections on areas of high risk, taking into account the impact of non-compliance; for example, unnecessary intrusion on an individual's privacy.

We assess compliance based on the records available, discussions with relevant agency teams, observations of agencies' processes through the information they provide, and the agency's remedial action in response to issues we or its staff identify. To maintain the integrity of active investigations, we do not inspect records relating to warrants and authorisations that are still in force.

To ensure the agency understands what we will be assessing, prior to each inspection we provide it with a broad outline of our criteria. This helps agency staff to identify the most accurate sources of information to assist our inspection.

We also encourage agencies to tell us about instances of non-compliance, including any remedial action they have taken.

At the end of each inspection we verbally advise the agency of our preliminary findings. This enables the agency to commence taking remedial action without waiting for our formal report. We may also provide agencies with feedback on their policies and procedures, including communicating 'best practice' approaches to demonstrating compliance, and engaging with staff outside the formal inspection process.

Our criteria

The objective of our inspections is to assess the extent of compliance with the Act by the agency and its law enforcement officers.

We use the following broad criteria to assess agency compliance:

1. Were surveillance devices used in accordance with the Act?
2. Were computer access activities conducted in accordance with the Act?
3. Is protected information properly managed?
4. Was the agency transparent and were reports properly made?

Further detail on our inspection criteria and methodology is provided in **Appendix A.**

How we report to the Minister

To ensure procedural fairness, we give each agency the opportunity to comment on our draft inspection findings. Once we have considered and, where appropriate, incorporated the agency's response the inspection results are considered finalised. The findings from these reports are then de-sensitised and consolidated into the Ombudsman's six-monthly report to the Minister.

We may also report on issues other than instances of non-compliance, such as the adequacy of an agency's policies and procedures to demonstrate compliance with the Act. We will not generally include administrative issues or instances of non-compliance where the consequences are negligible, for example when a warrant containing errors was not executed.

Australian Commission for Law Enforcement Integrity

We inspected the Australian Commission for Law Enforcement Integrity's (ACLEI) surveillance device records from 16 to 18 September 2019.[5] We did not identify any compliance or administrative issues.

Inspection details

We inspected all four surveillance device warrants issued to ACLEI that expired or were revoked during the period from 1 January to 30 June 2019. ACLEI advised our Office it did not destroy or retain any protected information during this period.

Progress since our previous inspection

In our previous report to the Minister in September 2019, we noted ACLEI had disclosed to our Office that it had not completed the record-keeping and reporting requirements for one warrant. ACLEI also disclosed, and our inspection confirmed a small number of inaccuracies in its reports to the Minister under s 49 of the Act. At this inspection we verified that ACLEI had addressed all of these issues.

[5] This inspection was conducted concurrently with inspections under other legislation.

Australian Criminal Intelligence Commission

We inspected the Australian Criminal Intelligence Commission's (ACIC) surveillance device records from 16 to 20 September 2019.

Inspection details

We inspected records of warrants and authorisations that expired during the periods from 1 July to 31 December 2018, and from 1 January to 30 June 2019. We also inspected records relating to the ACIC's management of protected information during these periods.

1 July to 31 December 2018		
Type of record	**Records made available**	**Records inspected[6]**
Surveillance device warrant	78	12 (15%)
Retrieval warrant	1	1 (100%)
Tracking device authorisation	17	4 (23%)
Retention of protected information	37	37 (100%)
1 January to 30 June 2019		
Type of record	**Records made available**	**Records inspected**
Surveillance device warrant	77	16 (20%)
Retrieval warrant	4	4 (100%)
Computer access warrant	1	1 (100%)
Tracking device authorisation	21	6 (28%)
Retention of protected information	15	15 (100%)
Destructions of protected information	44	44 (100%)

Progress since our previous inspection

We last included inspection results for the ACIC in our March 2019 report to the Minister. In that report we identified an issue with the statutory provisions on which the ACIC had relied in conducting surveillance activities under one warrant. We also noted that, for three tracking device authorisations that were given verbally, the ACIC

[6] Our usual practice is to inspect records of executed warrants and authorisations, where surveillance activities have occurred. It is common for agencies to be issued with warrants but to not execute them due to, for example, operational opportunity.

did not make a written record as soon as practicable and in accordance with the requirements of the Act. At our most recent inspection we verified that the ACIC had since made those records.

We did not note any further instances of either issue at this inspection.

Inspection findings

We did not identify any significant compliance issues and noted only a small number of instances of non-compliance that were administrative or low-risk in nature. Where we identified risks associated with the ACIC's forms and templates for tracking device authorisations and revoking warrants, the ACIC advised our Office that it had addressed these subsequent to the inspection. Below we have set out an instance disclosed by the ACIC where it used a surveillance device contrary to a condition stipulated on a warrant. We have also made a better practice suggestion to the ACIC to assist it to achieve compliance with the destruction provisions of the Act.

The ACIC is to be commended for its ongoing transparency with our Office and its high level of preparedness for our inspections. We also appreciated the ACIC providing our Office with free access to its electronic record keeping system.

ACIC Disclosure – remedial action after protected information was obtained outside of warrant conditions

What the Act provides

Section 18 of the Act specifies what a surveillance device warrant may authorise, subject to any conditions specified in the warrant.

What the ACIC disclosed

The ACIC disclosed one instance where it had taken remedial action as a result of a surveillance device being used contrary to a condition specified in the warrant. In this instance, the ACIC had sought and been given an extension on a previously issued warrant, which imposed the condition that one of the types of devices in use was to cease being used. The ACIC later identified that, although it had considered the affected device to be deactivated, the device had in fact collected protected information after the extension came into effect. As soon as it identified this, the ACIC ceased using the surveillance device and quarantined the protected information it had collected.

Finding – Protected information not destroyed as soon as practicable

What the Act requires

Section 46(1)(b) of the Act states that the chief officer of a law enforcement agency must cause to be destroyed any record or report as soon as practicable if they are satisfied that the record or report is no longer required for civil or criminal proceedings.

What we found

On 12 February 2019, the chief officer approved the destruction of protected information obtained under 26 surveillance device warrants and tracking device authorisations. At the time of the inspection, approximately seven months after the approval, the protected information had not yet been fully destroyed. In the instances we identified, the ACIC had not completed its quality assurance procedures to ensure all protected information had been identified for destruction. As a result, we could not be satisfied these destructions occurred 'as soon as practicable', as required by s 46 of the Act. We consider that the 'as soon as practicable' requirement is in place to mitigate any risks associated with accessing protected information that is no longer required.

What we suggested

We note that, while the ACIC has a number of thorough quality assurance procedures in place for identifying relevant information to be destroyed (including information held by partner agencies), the extensive enquiries it undertakes appear to significantly delay destroying protected information after the chief officer has approved its destruction.

We suggested that the ACIC considers re-ordering its processes to identify all relevant protected information that is no longer required prior to seeking the chief officer's approval for destruction. We also suggested that the ACIC considers performing its destruction procedures more frequently and in smaller numbers, to better comply with the destruction provisions. The ACIC advised that it would consider our suggestions during an upcoming review of its relevant procedures. We will continue to monitor this issue.

Australian Federal Police

We conducted two inspections of the Australian Federal Police's (AFP) surveillance device records, from 12 to 15 March 2019 and from 14 to 18 October 2019.

Inspection details

We inspected records of warrants and authorisations that expired during the periods from 1 January to 31 December 2018 (in March 2019), and from 1 January to 30 June 2019 (in October 2019). We also inspected records relating to the AFP's management of protected information during these periods.

1 January to 31 December 2018 – March inspection		
Type of record	**Records made available**	**Number of records inspected**
Surveillance device warrants	565	34 (6%)
Retrieval warrants	20	6 (30%)
Emergency authorisation	1	1 (100%)
Tracking device authorisation	22	11 (50%)
Destruction of protected information	504	27 (5%)
Retention of protected information	160	8 (5%)
1 January to 30 June 2019 – October inspection		
Type of record	**Records made available**	**Number of records inspected**
Surveillance device warrants	268	34 (13%)
Retrieval warrants	9	9 (100%)
Computer access warrants	2	2 (100%)
Tracking device authorisation	123	28 (23%)
Destruction of protected information	147	21 (14%)
Retention of protected information	245	50 (20%)

Progress since our previous inspections

We last included inspection results for the AFP in our September 2018 report to the Minister. At that time we noted the AFP had disclosed a small number of instances where it continued to obtain protected information from surveillance devices after the relevant warrant or tracking device authorisation expired. The AFP also told us about

the remedial action that it had taken to address the causes of the breach and quarantine the unauthorised protected information. We did not identify any similar instances during our most recent inspections.

In our September 2018 report we also highlighted a small number of instances where the AFP did not revoke retrieval warrants when the original grounds for the warrants ceased to exist. The AFP updated its processes in response to our findings. However, due to the retrospective nature of our inspections, we identified another two instances of the same issue at the March inspection. We did not identify any further instances at our October inspection.

We also previously noted instances where the AFP had not met the requirements in the Act for retaining and destroying protected information. However, we did not identify any similar instances at our March or October inspections.

Inspection findings

The most significant issues identified at both inspections were: the use and retrieval of surveillance devices without the proper authority; and lack of adherence to the Act's requirements for internally issued emergency and tracking device authorisations, where judicial or AAT oversight is not required. These issues are discussed below.

Additionally, at both inspections we identified a small number of errors or omissions in the AFP's reports to the Minister under s 49 of the Act. The AFP subsequently advised our Office it had sent amended reports to the Minister.

AFP disclosure – remedial action taken after unauthorised extraterritorial use of a surveillance device

What the Act requires

Part 5 of the Act sets out the circumstances in which an agency may carry out surveillance activities in a foreign country, including agreement by an appropriate consenting official of the foreign country.

What the AFP disclosed

At our October inspection, the AFP disclosed one instance where it had inadvertently used a surveillance device in a foreign country and consequently conducted extraterritorial surveillance without meeting the requirements of Part 5. The AFP advised that, within 48 hours of identifying this issue it had ceased collecting protected information extraterritorially and quarantined the affected protected information.

The AFP disclosed a second instance of a similar issue; however, as this warrant did not expire during the inspection period, we will assess it at our next inspection.

Finding – Application made for a tracking device authorisation instead of a retrieval warrant

What the Act provides

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 to investigate a relevant offence. Under s 39(6) of the Act, if the appropriate authorising officer gives a tracking device authorisation, the officer may also authorise the retrieval, without a warrant, of the tracking device to which the authorisation relates.

Section 39(9)(b) of the Act states that, for the purposes of obtaining a tracking device authorisation, the law enforcement officer must address in their relevant application the matters that would be required to be addressed if an application were being made for a surveillance device or retrieval warrant. Section 16(2)(f) of the Act states that when determining the application for a warrant, the issuing authority must have regard to any previous warrant sought under Division 2 of Part 2 of the Act.

Section 22 of the Act provides that a law enforcement officer may apply to an eligible Judge or to a nominated AAT member for a retrieval warrant in respect of a surveillance device that was lawfully installed under a surveillance device warrant or tracking device authorisation.

What we identified

At our March inspection, we identified that an application for a tracking device authorisation was applied for, and relied upon to retrieve a tracking device that had been previously installed under a surveillance device warrant. We also noted that the relevant application to the AFP authorising officer did not include details of the previous warrant.

In this instance, we concluded the AFP should have applied to an eligible judge or nominated AAT member for a retrieval warrant under s 22 to retrieve this device, rather than seeking a tracking device authorisation.

The AFP's response

The AFP advised it would seek internal legal advice on this issue. Nevertheless, we will continue to monitor this issue at future inspections.

Finding – Tracking devices retrieved without the proper authority

What the Act requires

As noted above, under s 39 of the Act an authorising officer may authorise the use and retrieval of the tracking device to which the tracking device authorisation relates without a warrant.

Section 40 of the Act requires that, as soon as practicable after an authorisation has been given, the authorising officer must make a record of having given that authorisation including if the authorisation authorises the retrieval of a tracking device. Under s 40(1)(h) of the Act, where the tracking device authorisation authorises the retrieval of a tracking device, the object or premises from which it is to be retrieved must be specified.

What we identified

At our October inspection, we identified two instances where the AFP appeared to have relied on written records of authorisations to retrieve tracking devices, despite the authorisations not specifically authorising their retrieval.

In the absence of this information on the written record of the authorisation, we could not be satisfied the tracking devices were retrieved with lawful authority. Subsequent to the inspection, the AFP advised it did not seek specific authorisation to retrieve these devices.

What we suggested and the AFP's response

We suggested the AFP update its written templates to include details of whether the tracking device authorisation also authorises its retrieval. In response, the AFP advised that it currently requires investigators to seek separate authorisations for the installation and retrieval of tracking devices; however, it is considering our suggestion to amend its relevant templates and streamline its processes.

Finding – Emergency authorisation records incorrectly made

What the Act provides

Under s 29 of the Act a law enforcement officer can apply for an emergency authorisation to use a surveillance device in urgent circumstances relating to a recovery order. Section 31 of the Act requires the authorising officer to record the emergency authorisation as soon as practicable after giving it. Section 32(2) of the Act provides that

an emergency authorisation may authorise anything that a surveillance device warrant may authorise.

What we identified

At our March inspection we identified an instance where, although the application for an emergency authorisation met all of the requirements of the Act, the written record made by the appropriate authorising officer was in the form of a tracking device authorisation under s 39 of the Act.

While we acknowledged the emergency/tracking device authorisation was not executed, we highlighted the significant risk posed by granting a written tracking device authorisation instead of an emergency authorisation. An emergency authorisation may authorise anything a surveillance device warrant may authorise, such as entry onto private property, while a tracking device authorisation is more limited. This may lead to surveillance device activities, and the associated intrusion on privacy, occurring without proper authority.

The AFP's response

Subsequent to the inspection the AFP advised this instance was the result of an administrative error. The AFP advised that it intends to expand the information provided in its authorising officers' training to clearly explain the differences between these two types of internally given authorisations, so staff are better supported to ensure the appropriate authorisation is given.

Finding – Tracking device authorisation not in relation to the investigation of a relevant offence

What the Act provides

Under s 39 of the Act, an authorising officer may authorise the use of a tracking device without a warrant to investigate a relevant offence. Under s 39(2) of the Act, if the law enforcement officer is a State or Territory law enforcement officer, a relevant offence does not include a State offence that has a federal aspect.

What we identified

At our October inspection, we identified two tracking device authorisations that were given under the Act in relation to an investigation of a territory-based offence, without any reference to a Commonwealth offence. In one of these instances, the AFP executed the tracking device authorisation and obtained protected information.

Based on the information available to us at the time of our inspection report, we could not be satisfied these two tracking device authorisations satisfied the requirements of s 39 of the Act in relation to the investigation of a relevant offence.

What we suggested and the AFP's response

We suggested the AFP quarantine any protected information obtained under the executed tracking device authorisation. The AFP advised it would implement our suggestion and update its procedural guidance to mitigate further similar errors.

At a subsequent inspection in March 2020 the AFP provided internal legal advice it had obtained on this issue. We will consider that advice when examining similar instances that may arise in future.

Finding – Extensions to warrants not sought nor authorised in a compliant manner

What the Act requires

Section 19(2) of the Act requires that an application to vary or extend a surveillance device warrant be made to an eligible judge or to a nominated AAT member, and must be accompanied by the original warrant. Under s 19(5) of the Act, where an application to extend or vary a warrant is granted, the eligible judge or nominated AAT member must endorse the new expiry date or other varied terms on the original warrant.

What we identified

At our March and October inspections, we identified a number of instances where the endorsement of an extension or variation of a warrant was completed on an adhesive label that was attached to the original warrant, instead of the details being directly recorded onto the original warrant. In these instances, we were unable to confirm compliance with the Act, as we could not determine if the original warrant was provided to the eligible judge or AAT member during the issuing of the extension or variation, and whether the adhesive label was attached at that time.

Furthermore, we noted two instances at our October inspection where adhesive labels were attached to the incorrect warrant.

We note that, previously, the AFP would stamp a template on the original warrant for the eligible judge or AAT member to complete. We consider that this process better

aligns with the requirements under s 19(5) of the Act and avoids some of the risks associated with using other practices.

What we suggested and the AFP's response

We suggested to the AFP that it seek legal advice to assure itself that the practice of using adhesive labels is compliant with the requirements of the Act.

We also suggested that the AFP update its relevant procedural guidance to ensure that adhesive labels are only affixed in the presence of the eligible judge or AAT member, to mitigate the risk of a label being attached to the wrong warrant. We also suggested that a better practice approach would be for the AFP to ensure that the eligible judge or AAT member signs across the edge of the label onto the original warrant, to increase the reliability of this practice.

In response, the AFP advised that it is satisfied the use of adhesive labels complies with the Act. It advised our Office that the labels are attached by the eligible Judge or AAT member, or by another party in their presence, at the time an extension or variation is sought. The AFP also advised that, as far as it is aware, eligible judges and AAT members are comfortable with this practice, and noted this approach has not led to any questions regarding the validity of warrants during court proceedings.

The AFP also advised that its labels should be signed across the edge by the eligible Judge or AAT member, and it will update its relevant procedural guidance to ensure labels are used appropriately and extensions and variations to warrants are authorised in a manner that complies with the Act.

Finding – Inaccurately reporting on whether a tracking device authorisation was executed

What the Act requires

Section 49 of the Act states that the chief officer of a law enforcement agency must, as soon as practicable after a warrant, emergency authorisation or tracking device authorisation ceases to be in force, make a report to the Minister and provide copies of the warrant or authorisation and other specified documents. The report must also state whether the warrant or authorisation was executed, and if so, give specific details.

The reporting obligations in the Act are an important transparency and accountability mechanism regarding an agency's covert surveillance device activities.

What we identified

At our October inspection, we identified one instance where the AFP's report to the Minister under s 49 of the Act stated that a tracking device had not been executed. However we located information on file that indicated tracking devices had been used under this authorisation. We advised the AFP that it should send an updated report to the Minister.

The AFP's response

Subsequent to the inspection, the AFP advised this was the result of an administrative error and it had sent an amended report to the Minister.

New South Wales Police Force

We inspected the New South Wales Police Force's (NSWPF) surveillance device records on 23 and 24 July 2019.

Inspection details

During the inspection we assessed the one warrant that expired during the period 1 July 2017 to 30 June 2018, and the four warrants and one retrieval warrant that expired or were revoked during the period 1 July 2018 to 30 June 2019. The NSWPF advised our Office it did not destroy or retain any protected information during these periods.

Progress since our previous inspection

We last included inspection results for the NSWPF in our September 2018 report to the Minister. In the report we noted a small number of instances where the NSWPF had not met all of its record-keeping requirements and its reporting obligations to the Minister. At this inspection we verified that the NSWPF had addressed these instances; however, we also identified some further problems with its ministerial reports under s 49 of the Act. As a result, we made a number of suggestions to the NSWPF, including reviewing its processes to ensure accurate and timely reporting on its activities under the Act.

Subsequent to our July 2019 inspection the NSWPF advised that it had either sent, or will send additional documents and amended reports to the Minister. It also advised it had updated some of its templates and registers to prevent recurrence of these issues. We note the NSWPF's responsiveness to these issues, and will continue to monitor the NSWPF's progress at future inspections.

We also suggested in our September 2018 report that the NSWPF update its internal guidance regarding retaining and destroying protected information. This suggestion resulted from a small number of instances we identified where the NSWPF had not complied with the relevant requirements of the Act. At our July 2019 inspection, the NSWPF disclosed that it was undertaking an internal audit of its destruction and retention records, based on new practices it had implemented. At that time it also disclosed two instances where it appeared that protected information obtained under two warrants should have, but had not been destroyed.

We will continue to monitor the NSWPF's progress in managing its historical protected information in accordance with the Act.

Inspection findings

In addition to the issues discussed above, following our inspection the NSWPF advised that it had updated its templates to correctly refer to a vehicle as a premises, as defined under s 6 of the Act, rather than as an object. This will ensure that the NSWPF meets the requirements in the Act regarding surveillance device warrants issued in respect of premises. We also identified another risk associated with calculating the period of effect of warrant, which is discussed below.

Identified risk – miscalculating the period of effect of a warrant

What the Act requires

Section 17(1A) of the Act states that a warrant may only be issued for a period of no more than 90 days, where the warrant is not issued in respect of an integrity operation.

What we found

We identified two instances where there was a discrepancy between the application and warrant in relation to the duration the warrant was to be in force. Namely, the warrants were issued for a day longer than the period that was applied for. In one of these instances, the warrant was issued for a period of 91 days, contrary to the limit imposed by s 17(1A) of the Act.

This issue seems to have occurred as a result of the particular wording of the NSWPF's surveillance device warrant templates, which state that a warrant is in force from a specific date and time until another specific date and time. This practice can raise compliance risks through incorrectly calculating the period of effect of a warrant.

While the Act states that a warrant may be in force for a period of no more than 90 days, the NSWPF could rely on s 65 of the Act to assert the validity of the warrant. Section 65 of the Act provides that despite a defect or irregularity to the warrant, the warrant still provides sufficient authority for the use of surveillance devices. However, if any protected information was obtained on the 91st day, we would consider it to have been collected without authority. Based on the records provided, the NSWPF did not obtain any protected information after 90 days.

What we suggested and the NSWPF's remedial action

We suggested that the NSWPF review the wording on its warrant templates and its approach to calculating the period of effect for a warrant. In response, the NSWPF advised that these errors occurred due to using a tool for calculating state-based warrants, which excludes the day on which a warrant is issued when reckoning the

period of effect. The NSWPF has subsequently updated its tool for determining the period of effect for Commonwealth warrants to prevent this error from reoccurring.

South Australia Police

We inspected the South Australia Police's surveillance device records on 3 and 4 September 2019.

Inspection details

We inspected the one warrant that expired during the period 1 July 2017 to 30 June 2018 and the two warrants that expired during the period 1 July 2018 to 30 June 2019. The South Australia Police advised our Office that it did not destroy or retain any protected information during these periods.

Previous issues

We last included inspection results for the South Australia Police in our September 2018 report to the Minister. In the report, we noted a small number of instances where the South Australia Police had not adhered to the requirements in the Act regarding destroying and retaining protected information.

At our September 2019 inspection, the South Australia Police advised it was in the process of reviewing its destruction and retention processes. We will continue to monitor the South Australia Police's management of historical protected information.

Inspection findings

At our September 2019 inspection, we identified a small number of errors and omissions in the South Australia Police's reports to the Minister under ss 49 and 50 of the Act. Subsequent to the inspection the South Australia Police advised it had provided amended reports and additional information to the Minister under s 49 of the Act, and will provide updated information in its next report to the Minister under s 50 of the Act. We did not identify any further compliance or administrative issues.

We found the South Australia Police's surveillance device records to contain a high level of detail, which greatly assisted our Office in forming our compliance assessments.

Victoria Police

We inspected the Victoria Police's surveillance devices records on 27 August 2019.

Inspection details

We inspected the one warrant that expired during the period 1 July 2017 to 30 June 2018 and the one tracking device authorisation that expired during the period 1 July 2018 to 30 June 2019. The Victoria Police advised our Office that it did not destroy or retain any protected information during these periods.

Previous issues

We last included inspection results for the Victoria Police in our September 2018 report to the Minister. In the report, we noted a small number of instances where the Victoria Police had not adhered to the destruction and retention requirements in the Act. Despite these instances, we were satisfied that the Victoria Police had adequate processes in place to ensure compliance with these requirements. As we were unable to assess the ongoing effectiveness of these processes at this inspection, we will continue to monitor the issue at future inspections.

We also reported on two warrants that were issued for a period longer than provided for under the Act. As these two warrants were not executed and were subsequently revoked, there were minimal risks associated with these errors. We did not note any further instances during our August 2019 inspection.

Inspection findings

At our August 2019 inspection, apart from two errors in the Victoria Police's reports to the Minister under s 49 of the Act, we did not identify any compliance or administrative issues. Subsequent to the inspection, the Victoria Police advised that it had provided the correct information to the Minister.

Appendix A—Inspection criteria and methodology

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

1. Were surveillance devices used in accordance with the Act?

1.1 Did the agency have the proper authority for the use and/or retrieval of the device?

1.1.1 What are the agency's procedures to ensure that surveillance device warrants, retrieval warrants, revocation warrants and authorisations, are properly applied for and are they sufficient?*	1.1.2 Were authorisations properly granted?*	1.1.3 What are the agency's procedures for seeking extensions and variations, and are they sufficient?*
1.1.4 What are the agency's procedures for revoking surveillance device and retrieval warrants, and are they sufficient?*		

1.2 Were surveillance devices used and/or retrieved in accordance with the authority of warrants and authorisations?

1.2.1 What are the agency's procedures to ensure the lawful use of surveillance devices, and are they sufficient?*	1.2.2 Does the agency have an auditable system for maintaining surveillance devices?	1.2.3 What are the agency's systems and /or records capturing the use of surveillance devices, and are they sufficient?*
1.2.4 What are the agency's procedures for ensuring warrant conditions are adhered to, and are they sufficient?*		

2. Were computer access activities conducted in accordance with the Act?

2.1 Did the agency have the proper authority for the doing of certain things in relation to computer access?

2.1.1 What are the agency's procedures to ensure computer access warrants are properly applied for, and are they sufficient?*	2.1.2 What are the agency's procedures for seeking extensions and variations to computer access warrants, and are they sufficient?*	2.1.3 What are the agency's procedures for ensuring discontinuance of access under a computer access warrant, and are they sufficient?*
2.1.4 What are the agency's procedures for revoking computer access warrants, and are they sufficient?*		

2.2 Were computer access activities conducted in accordance with the authority of warrants?

2.2.1 What are the agency's procedures to ensure the lawful doing of things under a computer access warrant, and are they sufficient?*	2.2.2 What are the agency's systems and/or records capturing the things done under a computer access warrant, and are they sufficient?*	
2.2.3 What are the agency's procedures for ensuring computer access warrant conditions are adhered to, and are they sufficient?*		

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

2.3.1 Did the chief officer of the relevant law enforcement agency notify the Ombudsman in relation to 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, and in accordance with the Act?

3. Is protected information properly managed?

3.1 Is protected information properly stored, used and disclosed?

3.1.1 What are the agency's procedures for ensuring the secure storage of protected information, and are they sufficient?*	3.1.2 What are the agency's procedures for ensuring the proper use and disclosure of information, and are they sufficient?*
3.1.3 What are the agency's procedures for ensuring the protection of privacy?	

3.2 Was protected information properly destroyed and/or retained?

3.2.1 What are the agency's procedures for ensuring that protected information is destroyed in accordance with the Act, and are they sufficient?*	3.2.2 What are the agency's procedures for ensuring that protected information is retained in accordance with the Act, and are they sufficient?*
3.2.3 Does the agency regularly review its protected information to ensure compliance with the Act?	

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

4.1 Were all records kept in accordance with the Act?

4.1.1 What are the agency's record keeping procedures, and are they sufficient?*

4.2 Were reports properly made?

4.2.1 What are the agency's procedures for ensuring that it accurately reports to the Minister (Department of Home Affairs) and the Commonwealth Ombudsman, and are they sufficient?*

4.3 Was the agency cooperative and frank?

Considerations may include:

- Does the agency have a culture of compliance?
- Was the agency proactive in identifying compliance issues?
- Did the agency disclose issues before or during an inspection?
- Were issues identified at previous inspection/s addressed by the agency?
- Has the agency engaged with the Commonwealth Ombudsman's office, as necessary?

* Sufficiency will be tested through secondary checks such as corroborating records.