victorian inspectorate

Inspection Report:

Surveillance Devices Act 1999 (Vic)

Report by the Victorian Inspectorate on surveillance device records inspected during the period 1 January 2019 to 30 June 2019

Contents

Overview

This report presents the results of the inspections conducted by the Victorian Inspectorate ('the VI') between 1 January to 30 June 2019 of records belonging to the following five Victorian agencies authorised to use surveillance devices:

- Department of Environment, Land, Water and Planning (DELWP)
- Game Management Authority (GMA)
- Independent Broad-based Anti-corruption Commission (IBAC)
- Victorian Fisheries Authority (VFA)
- Victoria Police

The *Surveillance Devices Act* 1999 (Vic) ('the SD Act') provides the legislative framework for these agencies to use surveillance devices to investigate, or obtain evidence of the commission of, an offence that has been, is being, is about to be, or is likely to be, committed. Law enforcement officers of these agencies can apply to the Supreme Court for a surveillance device warrant with respect to the following types of devices: data; listening; optical; and tracking. For tracking devices only, an application may also be made to the Magistrates' Court. Victoria's Public Interest Monitor (PIM) is entitled to make submissions on warrant applications. In addition to court-issued warrants, senior officers of Victoria Police and IBAC can, in certain emergency situations, authorise the use of surveillance devices.

The role of the VI is established by the SD Act, and ensures independent oversight of the above agencies with respect to compliance with the Act. The VI is required to inspect from time to time the records of each agency, and report on the results of its inspections at 6-monthly intervals to each House of Parliament as well as the Attorney-General. The use of surveillance devices by Victorian government agencies is highly intrusive of individuals' privacy, and therefore the VI's role is designed to assure the public that the lawfulness of agency actions is subject to independent checks.

The VI notes in this report the cooperative and transparent engagement by the officers of each agency whose records were subject to our inspection. Whilst the VI reports on some minor errors in record keeping, no significant compliance issues were identified. The VI commends the remedial actions taken by agencies to address the identified errors.

The VI has not made any recommendations as a result of its inspections of surveillance device records for the 1 January to 30 June 2019 reporting period.

Introduction

The SD Act imposes strict controls on the use of surveillance devices by Victorian law enforcement agencies, including the use and communication of information obtained by the use of such devices, and reporting obligations. It also imposes requirements for the secure storage and destruction of records or reports containing information obtained by the use of surveillance devices.

OUR ROLE

The VI performs an independent oversight function to determine the extent of compliance achieved by law enforcement agencies that have exercised their powers under the SD Act.

The VI is required to inspect the records of these agencies from time to time to determine the extent of compliance with the SD Act. In order to fulfil our requirement to report to Parliament at 6-monthly intervals, the VI conducts biannual inspections of:

- surveillance device warrants;
- emergency authorisations; and
- retrieval warrants;

which had ceased during the period.

The VI inspects hard copy documents and electronic registers with the primary purpose of ensuring that records connected with the issue of surveillance device warrants, and other records connected with the use of devices, are being kept. The VI will also confirm that each law enforcement agency has met its prescribed reporting obligations.

HOW WE ASSESS COMPLIANCE

The objective of our inspections is to determine the extent of compliance with the SD Act by each Victorian law enforcement agency authorised to use surveillance devices, and that of their officers. We assess compliance based on the records made available to us at the time of inspection, our discussions with the relevant agencies, as well as the action they take in response to any issues we have raised.

HOW WE REPORT ON COMPLIANCE

To ensure procedural fairness, each agency is given an opportunity to comment on the VI's findings from our inspections, and to furnish additional records that might assist our assessment. Following this process, the inspection results are considered finalised.

Included in this report are findings resulting from our inspection and assessment of records and documents relating to the issue and use of surveillance device warrants and authorisations by Victorian law enforcement agencies. We provide more detail where there is a finding of non-compliance. The VI may, in its discretion, not report on administrative issues (such as typographical or transposition errors) or instances of non-compliance where the consequences are negligible.

The following sections of this report provide the results of the VI's inspection of surveillance records from 1 January to 30 June 2019. Inspection results are reported on separately for each Victorian law enforcement agency with the authority to exercise powers under the SD Act.

Department of Environment Land Water and Planning

The Department of Environment Land Water and Planning (DELWP)'s 'Intelligence and Investigations Unit' administers surveillance device warrants issued to the agency.

The VI inspected one (1) surveillance device file at DELWP on 30 April 2019. This was the only surveillance device warrant issued to DELWP that ceased between 1 July and 31 December 2018.

FINDINGS – WARRANTS

Were applications for warrants (including extensions and variations) properly made?

The VI found that the application made for a surveillance device warrant by DELWP complied with the requirements of s 15 of the SD Act.

Specifically, the VI found the following application requirements were met:

- Approval was provided by a senior officer.
- The applicant was a law enforcement officer.
- The applicant's name as well as the nature and duration of the warrant were specified, including the type of device sought.
- A sworn affidavit was provided in support.
- The application was made to an appropriate court.

DEWLP made no applications for the inspected warrant to be extended or varied.

Were warrants in proper form and revocations properly made?

Issued warrants must specify the following matters in accordance with s 18 of the SD Act:

- The name of the applicant and alleged offence.
- Date warrant was issued and the kind of surveillance device authorised.
- The permitted premises, object or class of object for the device, as applicable.
- Name of person whose conversations or movements will be subject to the device, if known.
- Duration for the warrant (up to 90 days).
- Name of primary law enforcement officer responsible for executing the warrant.
- Any conditions for the installation or use of the device.
- When the report made under s 30K of the SD Act must be made.
- The name and signature of the issuing authority (magistrate or judge).

The warrant issued to DELWP met all of these requirements.

DELWP discontinued the use of a surveillance device and subsequently revoked the corresponding warrant via a written instrument signed by the chief officer (Secretary), in accordance with ss 20A and 20B of the SD Act.

FINDINGS – RECORDS

Did DELWP keep all records connected with warrants?

DELWP is required to keep certain records in connection with surveillance device warrants, including:

- Each warrant issued.
- A copy of each warrant application, and any application for its extension, variation or revocation.
- A copy of each report made under s 30K of the SD Act to a magistrate or judge.
- Copies of any evidentiary certificates issued under s 36 of the SD Act.

DELWP complied with these record-keeping requirements, with the exception of keeping the original warrant issued.

Finding 1 – Original warrant not kept on file.

DELWP is required to keep the original warrant, amongst other documents, on file. In the one file inspected from 1 January to 30 June 2019, a copy only for the warrant issued was found to be kept on file.

DELWP confirmed that, at the direction of staff at the Magistrate's Court of Victoria (MCV) at the time it was issued, the original warrant was retained at the Court. DELWP has subsequently made a commitment to retain all original warrants issued to them in the future.

Whilst the absence of the original warrant means the requirement of s 30M(a) of the SD Act was not met, the VI accepts that DELWP officers were following the instruction of staff of the MCV, and that it will ensure in future that original warrants issued to it are held at DELWP.

Did DELWP keep all other necessary records?

DELWP is also required to keep other records, including details of:

- Each use made of information obtained by a surveillance device.
- Each communication of information obtained by the use of a surveillance device to a person other than a DELWP law enforcement officer.
- Each occasion information obtained by a surveillance device was given in evidence in a relevant proceeding.
- The destruction of records or reports obtained by the use of surveillance devices.

The VI found that DELWP complied with these requirements.

Did DELWP maintain an accurate register of warrants?

The VI found that a register of warrants was kept by DELWP, as required by s 30O(1) of the SD Act.

The register specified, with respect to the one (1) warrant file inspected, the following particulars:

- Date the warrant was issued.
- Name of magistrate who issued the warrant, as well as the name of the primary law enforcement officer responsible for its execution.
- The offence in relation to which the warrant was issued.
- The period during which the warrant was in force.

FINDINGS – REPORTS

Were reports on warrants properly made?

DELWP is required, within the time specified in the warrant, to make a report to the magistrate or judge who issued the surveillance device warrant. Each report must state whether the warrant was executed; and if it was, to give the following details for its use:

- Name of each person who executed the warrant.
- Kind of surveillance device used.
- Period the device was used.
- Name of any person whose movements or conversations were captured by use of the device or geographic location determined by a tracking device, if known.
- Premises for installation of the device or the location for its use, as applicable.
- Object in or on which the device was installed or the premises for such object, as applicable.
- The benefit to the investigation as well as the general use made or to be made of the information derived from its use.
- Compliance with any warrant conditions, as applicable.
- If the warrant was extended or varied, the number of such occurrences and the reasons for them.
- If the warrant was revoked by the chief officer under s 20A(2), whether the Public Interest Monitor was notified of this and the reasons the device was no longer required.

The one (1) report made by DELWP for the warrant that ceased between 1 July and 31 December 2018 was made within the requisite timeframe and complied with the above-mentioned requirements under ss 30K(1)-(2) of the SD Act.

FINDINGS - TRANSPARENCY AND COOPERATION

The VI considers an agency's transparency, its cooperation during inspection, and its responsiveness to suggestions and issues to be a measure of its compliance culture.

Did DELWP self-disclose compliance issues?

DELWP did not make any self-disclosures relevant to the warrant file inspected during 1 January to 30 June 2019.

Were issues identified at previous inspections addressed?

Since DELWP had no surveillance device warrant files requiring inspection during the previous reporting period, there were no historical issues to be addressed.

Game Management Authority

The Game Management Authority (GMA) has yet to make an application under the SD Act, and as a result no files were inspected by the VI between 1 January and 30 June 2019.

Independent Broad-based Anti-corruption Commission

The Independent Broad-based Anti-corruption Commission (IBAC)'s 'Legal Compliance Unit' administers surveillance device warrants issued to it. The VI inspected 2 surveillance device files at IBAC on 20 May 2019, which constituted all relevant records associated with warrants that ceased between 1 July 2018 and 31 December 2018.

FINDINGS – WARRANTS

Were applications for warrants (including extensions and variations) properly made?

The VI found that the 2 applications made for a surveillance device warrant by IBAC complied with the requirements of s 15 of the SD Act.

Specifically, the VI found the following application requirements were met:

- Approval was provided by a senior officer.
- Applicants were law enforcement officers.
- The applicant's name as well as the nature and duration of each warrant were specified, including the type of device sought.
- Sworn affidavits were provided in support.
- Applications were made to appropriate courts.

IBAC made no applications for the inspected warrants to be extended or varied.

Were warrants and emergency authorisations in proper form and revocations properly made?

Issued warrants must specify the following matters in accordance with s 18 of the SD Act:

- The name of the applicant and alleged offence.
- Date warrant was issued and the kind of surveillance device authorised.
- The permitted premises, object or class of object for the device, as applicable.
- Name of person whose conversations or movements will be subject to the device, if known.
- Duration for the warrant (up to 90 days).
- Name of primary law enforcement officer responsible for executing the warrant.
- Any conditions for the installation or use of the device.
- When the report made under s 30K of the SD Act must be made.
- The name and signature of the issuing authority (magistrate or judge).

The 2 warrants issued to IBAC met all of these requirements.

IBAC did not exercise the provisions under ss 20A and 20B of the SD Act to discontinue and revoke any warrant inspected.

IBAC did not make any emergency authorisations for the use of a surveillance device in the period.

FINDINGS –RECORDS

Did IBAC keep all records connected with warrants and emergency authorisations?

IBAC is required to keep certain records in connection with surveillance device warrants, including:

- Each warrant issued.
- A copy of each warrant application, and any application for its extension, variation or revocation.
- A copy of each report made under s 30K of the SD Act to a magistrate or judge.
- Copies of any evidentiary certificates issued under s 36 of the SD Act.

IBAC complied with these record-keeping requirements, noting no application was made for an emergency authorisation.

Did IBAC keep all other necessary records?

IBAC is also required to keep other records, including details of:

- Each use made of information obtained by a surveillance device.
- Each communication of information obtained by the use of a surveillance device to a person other than an IBAC law enforcement officer.
- Each occasion information obtained by a surveillance device was given in evidence in a relevant proceeding.
- The destruction of records or reports obtained by the use of surveillance devices.

The VI found that IBAC complied with these requirements, including keeping details of the destruction of records associated with 5 warrants.

At the May 2019 inspection IBAC advised the VI that it had changed its approval procedure for destroying records obtained by the use of surveillance devices. IBAC has considered the obligation on the IBAC Commissioner to authorise the destruction of information, and decided that it can be acquitted by the Team Leader in the Legal Compliance Unit, based on the principle that this activity is of a reasonably routine administrative nature and does not require the personal attention of the IBAC Commissioner. Under this implied agency, information is destroyed for and on behalf of the IBAC Commissioner. The VI will seek further information regarding this change to IBAC's destructions process at its next inspection to ensure the requirements under the SD Act are being satisfied.

Did IBAC maintain an accurate register of warrants and emergency authorisations?

The VI found that a register of warrants was kept by IBAC, as required by s 30O(1) of the SD Act.

The register specified, with respect to each warrant file inspected, the following particulars:

- Date the warrant was issued.
- Name of judge who issued the warrant, as well as the name of the primary law enforcement officer responsible for its execution.
- The offence in relation to which the warrant was issued.
- The period during which the warrant was in force.

Since IBAC did not exercise its emergency authorisation powers with respect to the inspected files there were no further matters to be specified in the register.

FINDINGS – REPORTS

Were reports on warrants properly made?

IBAC is required, within the time specified in the warrant, to make a report to the magistrate or judge who issued the surveillance device warrant. Each report must state whether the warrant was executed; and if it was, to give the following details for its use:

- Name of each person who executed the warrant.
- Kind of surveillance device used.
- Period the device was used.
- Name of any person whose movements or conversations were captured by use of the device or geographic location determined by a tracking device, if known.
- Premises for installation of the device or the location for its use, as applicable.
- Object in or on which the device was installed or the premises for such object, as applicable.
- The benefit to the investigation as well as the general use made or to be made of the information derived from its use.
- Compliance with any warrant conditions, as applicable.
- If the warrant was extended or varied, the number of such occurrences and the reasons for them.
- If the warrant was revoked by the chief officer under s 20A(2), whether the Public Interest Monitor was notified of this and the reasons the device was no longer required.

The 2 reports made by IBAC for warrants that ceased between 1 July and 31 December 2018 were made within the requisite timeframe and complied with the above-mentioned requirements under ss 30K(1)-(2) of the SD Act.

FINDINGS - TRANSPARENCY AND COOPERATION

The VI considers an agency's transparency, its cooperation during inspection, and its responsiveness to suggestions and issues to be a measure of its compliance culture.

Did IBAC self-disclose compliance issues?

IBAC did not make any self-disclosures relevant to warrant files inspected from 1 January to 30 June 2019.

Were issues identified at previous inspections addressed?

Since no issues with IBAC files were identified from the VI inspection conducted during the previous reporting period, there were no historical issues to be addressed on this occasion.

Victorian Fisheries Authority

The VI inspected 2 surveillance device files at Victorian Fisheries Authority (VFA) on 16 April 2019. Unlike the files of other agencies inspected from 1 January to 30 June 2019, the VFA surveillance warrants ceased after 31 December 2018. No surveillance device warrants issued to VFA ceased between 1 July and 31 December 2018.

FINDINGS – WARRANTS

Were applications for warrants (including extensions and variations) properly made?

The VI found that both applications made for a surveillance device warrant by VFA complied with the requirements of s 15 of the SD Act.

Specifically, the VI found the following application requirements were met:

- Approval was provided by a senior officer.
- Applicants were law enforcement officers.
- The applicant's name as well as the nature and duration of the warrant were specified, including the type of device sought.
- A sworn affidavit was provided in support.
- Applications were made to appropriate courts.

VFA made no applications for the inspected warrants to be extended or varied.

Were warrants in proper form and revocations properly made?

Issued warrants must specify the following matters in accordance with s 18 of the SD Act:

- The name of the applicant and alleged offence.
- Date warrant was issued and the kind of surveillance device authorised.
- The permitted premises, object or class of object for the device, as applicable.
- Name of person whose conversations or movements will be subject to the device, if known.
- Duration for the warrant (up to 90 days).
- Name of primary law enforcement officer responsible for executing the warrant.
- Any conditions for the installation or use of the device.
- When the report made under s 30K of the SD Act must be made.
- The name and signature of the issuing authority (magistrate or judge).

The warrants issued to VFA met all of these requirements.

Whilst one warrant was not executed, the VFA discontinued use of the surveillance device for the other and subsequently revoked both warrants via a written instrument signed by the chief officer (Secretary), in accordance with ss 20A and 20B of the SD Act.

FINDINGS –RECORDS

Did VFA keep all records connected with warrants?

VFA is required to keep certain records in connection with surveillance device warrants, including:

- Each warrant issued.
- A copy of each warrant application, and any application for its extension, variation or revocation.
- A copy of each report made under s 30K of the SD Act to a magistrate or judge.
- Copies of any evidentiary certificates issued under s 36 of the SD Act.

VFA complied with these record-keeping requirements, although the VI was unable to confirm for one (1) inspected file the VFA had kept the original surveillance device warrant issued since a copy of the warrant rather than the original was provided at time of inspection. VFA advised the VI shortly after the inspection the original warrant had been returned to the file. To confirm compliance with this record-keeping requirement, the VI will re-inspect this warrant file at the next scheduled inspection.

Did VFA keep all other necessary records?

VFA is also required to keep other records, including details of:

- Each use made of information obtained by a surveillance device.
- Each communication of information obtained by the use of a surveillance device to a person other than a VFA law enforcement officer.
- Each occasion information obtained by a surveillance device was given in evidence in a relevant proceeding.
- The destruction of records or reports obtained by the use of surveillance devices.

The VI found that VFA complied with these requirements, with the exception of how the use made of information obtained by a surveillance device was recorded for one (1) issued warrant.

Finding 1 – Incorrect recording of use made of information from surveillance device.

VFA communications register recorded one (1) surveillance device warrant was used to *"support mobile surveillance, observations and evidence gathering"* as well as *"identification of place and persons of interest potentially involved in the trafficking of priority species"*. The report made to the magistrate under s 30K of the SD Act for the corresponding warrant recorded nil uses however for information obtained by the surveillance device.

Following further enquiries with VFA, it was confirmed the communications register recorded anticipated, rather than actual, uses for information obtained by the device. The report therefore correctly stated that nil use was made of information obtained from the surveillance device. VFA subsequently corrected the entry in its communications register for this warrant.

VFA additionally notified their communications register has been amended to make it clear that only actual uses for information obtained from surveillance devices be recorded. The VI will re-inspect this warrant file at the next scheduled inspection.

The VI noted that although the VFA's communications register recorded the names of persons who had received information obtained by surveillance devices, it was not apparent from the register whether information had been communicated to a person other than a VFA law enforcement officer.

The VI suggested to VFA that best practice would be to amend the communications register template so that each communication entered includes details of which agency the recipient of the information belongs to.

Following the inspection, VFA confirmed that it has implemented this best practice suggestion.

Did VFA maintain an accurate register of warrants?

The VI found that a register of warrants was kept by VFA, as required by s 30O(1) of the SD Act.

The register specified, with respect to each warrant file inspected, the following particulars:

- Date the warrant was issued.
- Name of magistrate or judge who issued the warrant, as well as the name of the primary law enforcement officer responsible for its execution.
- The offence in relation to which the warrant was issued.
- The period during which the warrant was in force.

FINDINGS – REPORTS

Were reports on warrants properly made?

VFA is required, within the time specified in the warrant, to make a report to the magistrate or judge who issued the surveillance device warrant. Each report must state whether the warrant was executed; and if it was, to give the following details for its use:

- Name of each person who executed the warrant.
- Kind of surveillance device used.
- Period the device was used.
- Name of any person whose movements or conversations were captured by use of the device or geographic location determined by a tracking device, if known.
- Premises for installation of the device or the location for its use, as applicable.
- Object in or on which the device was installed or the premises for such object, as applicable.
- The benefit to the investigation as well as the general use made or to be made of the information derived from its use.
- Compliance with any warrant conditions, as applicable.

- If the warrant was extended or varied, the number of such occurrences and the reasons for them.
- If the warrant was revoked by the chief officer under s 20A(2), whether the Public Interest Monitor was notified of this and the reasons the device was no longer required.

The 2 reports made by VFA for the inspected warrants were made within the requisite timeframe and complied with the above-mentioned requirements under ss 30K(1)-(2) of the SD Act.

FINDINGS - TRANSPARENCY AND COOPERATION

The VI considers an agency's transparency, its cooperation during inspection, and its responsiveness to suggestions and issues to be a measure of its compliance culture.

Did VFA self-disclose compliance issues?

VFA did not make any self-disclosures.

Were issues identified at previous inspections addressed?

Since no issues with VFA files were identified from the VI inspection conducted during the previous reporting period, there were no historical issues to be addressed.

The VFA was responsive and transparent during the inspection process, in particular where the VI raised questions about certain records.

The VI notes that VFA accepted its best practice suggestion with regards to recording whether information obtained by the use of a surveillance device had been communicated internally (i.e., with a VFA law enforcement officer) or externally (refer to page 15 of this report) and quickly implemented a change to its communications register to reflect this best practice between the inspection and the drafting of this report.

Victoria Police

There are two units within Victoria Police that administer surveillance device warrants and emergency authorisations:

- The Special Projects Unit (SPU), the major user of surveillance device warrants; and
- The Technical Projects Unit (TPU), which resides within Professional Standards Command (PSC).

In addition to these units, the Technical Surveillance Unit (TSU) within Victoria Police is responsible for the installation, maintenance and retrieval of surveillance devices under the authority of warrants or emergency authorisations. Records held by the TSU in relation to these matters as well as the destruction of records and reports obtained by the use of surveillance devices were inspected on 6 June 2019, and were cross-checked against records held by the SPU and TPU.

The VI inspected a total of 45 surveillance device files with Victoria Police during the period. The inspected files related to 44 surveillance device warrants (including one (1) with a variation made to a condition) and one (1) emergency authorisation, all of which ceased between 1 July 2018 and 31 December 2018. There were 4 surveillance device files at the TPU inspected on 1 April 2019, and 41 files at the SPU inspected from 2-3 April 2019.

FINDINGS – WARRANTS

Were applications for warrants (including extensions and variations) properly made?

The VI found that all applications made for a surveillance device warrant, including a variation to a warrant, complied with the requirements of ss 15 and 20 of the SD Act.

Specifically, the VI found the following warrant application requirements were met:

- Approval was provided by an authorised police officer.
- The applicants were law enforcement officers.
- The applicant's name as well as the nature and duration of the warrant were specified, including the type of device sought.
- A sworn affidavit was provided in support.
- The applications were made to appropriate courts.

In addition to the above-mentioned requirements, applications for warrant extensions and variations also complied with the following:

- Extensions were sought for a period not exceeding 90 days.
- Each application was made to the same court (Supreme or Magistrates) that issued the initial warrant.

Were warrants and emergency authorisations in proper form and revocations properly made?

Issued warrants must specify the following matters in accordance with s 18 of the SD Act:

- The name of the applicant and alleged offence.
- Date warrant was issued and the kind of surveillance device authorised.
- The permitted premises, object or class of object for the device, as applicable.
- Name of person whose conversations or movements will be subject to the device, if known.
- Duration for the warrant (up to 90 days).
- Name of primary law enforcement officer responsible for executing the warrant.
- Any conditions for the installation or use of the device.
- When the report made under s 30K of the SD Act must be made.
- The name and signature of the issuing authority (magistrate or judge).

The 44 warrants issued to Victoria Police complied with these requirements.

Victoria Police discontinued use of 33 surveillance devices and subsequently revoked the associated warrants via written instruments signed by a delegate of the Chief Commissioner of Police, in accordance with ss 20A and 20B of the SD Act.

Victoria Police made one (1) emergency authorisation for use of a surveillance device during an investigation into a serious drug offence. Following application by a law enforcement officer, the authorisation was made by a senior officer.

An application for approval to exercise powers under the emergency authorisation was made to a Supreme Court judge within 2 business days of the authorisation and included:

- The applicant's name.
- Details of kind of surveillance device sought.
- A sworn affidavit was provided in support.

There was no requirement for the application to specify the nature and duration of the warrant, as no warrant was sought on this occasion.

FINDINGS –RECORDS

Did Victoria Police keep all records connected with warrants and emergency authorisations?

Victoria Police is required to keep certain records in connection with surveillance device warrants, including:

- Each warrant issued.
- Each emergency authorisation, and application made for such.
- A copy of each warrant application, and any application for its extension, variation or revocation.
- A copy of each application for approval to exercise powers under an emergency authorisation.
- A copy of each report made under s 30K of the SD Act to a magistrate or judge.

- Copies of any evidentiary certificates issued under s 36 of the SD Act.

Victoria Police complied with these record-keeping requirements.

Did Victoria Police keep all other necessary records?

Victoria Police is also required to keep other records, including details of:

- Each use made of information obtained by a surveillance device.
- Each communication of information obtained by the use of a surveillance device to a person other than a Victoria Police law enforcement officer.
- Each occasion information obtained by a surveillance device was given in evidence in a relevant proceeding.
- The destruction of records or reports obtained by the use of surveillance devices.

The VI found that Victoria Police complied with these requirements, including keeping details on the destruction of records and reports related to 33 surveillance device warrants.

Did Victoria Police maintain an accurate register of warrants and emergency authorisations?

The VI found that a register of warrants was kept by Victoria Police, as required by s 30O(1) of the SD Act.

The register specified, with respect to each warrant file inspected, the following particulars:

- Date the warrant was issued.
- Name of magistrate or judge who issued the warrant, as well as the name of the primary law enforcement officer responsible for its execution.
- The offence in relation to which the warrant was issued.
- The period during which the warrant was in force.

In relation to one (1) emergency authorisation, the register further specified the following matters in accordance with s 30O(3) of the SD Act:

- Date emergency authorisation was given.
- Name of senior officer who gave the authorisation, as well as the law enforcement officer who received it.
- The offence connected to the authorisation.
- Date application was made (to the Supreme Court) for approval of powers exercised under the emergency authorisation.

FINDINGS – REPORTS

Were reports properly made?

Victoria Police is required, within the time specified in the warrant, to make a report to the magistrate or judge who issued the surveillance device warrant. Each report must state whether the warrant was executed; and if it was, to give the following details for its use:

- Name of each person who executed the warrant.
- Kind of surveillance device used.
- Period the device was used.
- Name of any person whose movements or conversations were captured by use of the device or geographic location determined by a tracking device, if known.
- Premises for installation of the device or the location for its use, as applicable.
- Object in or on which the device was installed or the premises for such object, as applicable.
- The benefit to the investigation as well as the general use made or to be made of the information derived from its use.
- Compliance with any warrant conditions, as applicable.
- If the warrant was extended or varied, the number of such occurrences and the reasons for them.
- If the warrant was revoked by the chief officer under s 20A(2), whether the Public Interest Monitor was notified of this and the reasons the device was no longer required.

All reports made by Victoria Police for warrants that ceased between 1 July and 31 December 2018 were made within the requisite timeframe and complied with the above-mentioned requirements under ss 30K(1)-(2) of the SD Act.

FINDINGS - TRANSPARENCY AND COOPERATION

The VI considers an agency's transparency, its cooperation during inspection, and its responsiveness to suggestions and issues to be a measure of its compliance culture.

Did Victoria Police self-disclose compliance issues?

Victoria Police did not make any self-disclosures at inspections during the period.

Were issues identified at previous inspections addressed?

Victoria Police's SPU addressed one (1) issue identified at the previous inspection relating to an omission of a general use made of information derived from a surveillance device in the s 30K report by filing an amended report.