



Inspection Report:

Surveillance Devices Act 1999 (Vic)

Report by the Victorian Inspectorate on surveillance device records inspected during the period 1 July 2019 to 31 December 2019

Contents

Overview	1
Introduction.....	2
OUR ROLE	2
HOW WE ASSESS COMPLIANCE	2
HOW WE REPORT ON COMPLIANCE	3
Department of Environment Land Water and Planning	4
FINDINGS – WARRANTS	4
FINDINGS – RECORDS.....	5
FINDINGS – REPORTS	6
FINDINGS - TRANSPARENCY AND COOPERATION	7
Game Management Authority	9
Independent Broad-based Anti-corruption Commission	10
FINDINGS – WARRANTS	10
FINDINGS – RECORDS.....	11
FINDINGS – REPORTS	12
FINDINGS - TRANSPARENCY AND COOPERATION	12
Victorian Fisheries Authority	14
Victoria Police	15
FINDINGS – WARRANTS	15
FINDINGS – RECORDS.....	16
FINDINGS – REPORTS	17
FINDINGS - TRANSPARENCY AND COOPERATION	18

Overview

This report presents the results of the inspections conducted by the Victorian Inspectorate ('the VI') between 1 July to 31 December 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 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 July to 31 December 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 ceased during the preceding 6-monthly 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.

In this report, we also assess compliance with the reporting requirements of s 30L of the SD Act. Each agency able to make applications to use a surveillance device is required to make an annual report to the responsible Minister (Attorney-General) that is also tabled in Parliament. The VI assesses these reports against various criteria, including the requirement they be submitted to the Attorney-General by 30 September each year.

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 July to 31 December 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 3 surveillance device files at DELWP on 31 October 2019. These files represented all surveillance device warrants issued to DELWP that ceased between 1 January and 30 June 2019.

FINDINGS – WARRANTS

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

The VI found that DELWP's applications for surveillance device warrants complied with the requirements of s 15 of the SD Act.

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

- 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 a Supreme Court judge or magistrate, as appropriate.

DELWP made 2 separate applications for a warrant to be extended and in each case the following additional requirements were complied with:

- Extensions were sought for a period not exceeding 90 days.
- Each application was made to a Supreme Court judge or magistrate, depending on which level of the judiciary issued the warrant.

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 of the warrant (up to 90 days).
- The name of the primary law enforcement officer responsible for executing the warrant.
- Any conditions for the installation or use of the device.
- When the report 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 DELWP met all of these requirements.

DELWP discontinued the use of surveillance devices and subsequently revoked all 3 warrants it was issued with via written instruments 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 issued warrant in 2 instances.

Finding 1 – Original warrants not kept on file.

DELWP is required to keep the original warrant, amongst other documents, on file. In 2 inspected files a copy of the warrant issued, not the original, was kept. DELWP advised that in both cases the original issued warrant was retained at the Court at the direction of staff at the Magistrate's Court of Victoria (MCV) at the time it was issued.

Although this issue was raised by the VI at our previous inspection, these surveillance device warrant applications were made prior to the last inspection. The continued reporting of this issue therefore does not reflect any inadequacy by DELWP to address the earlier raising of this issue.

DELWP has advised it will seek 2 original warrants on each future surveillance device warrant application it makes at the MCV so that an original issued warrant can be retained in accordance with s 30M(a) of the SD Act.

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. The VI identified an error in the information recorded in the electronic register about the use made of information obtained by a surveillance device for one (1) warrant. DELWP confirmed that the information it had reported to the magistrate under s 30K of the SD Act correctly recorded the use that was made and amended the electronic register accordingly.

Did DELWP maintain an accurate register of warrants?

DELWP is required by s 30O(1) of the SD Act to keep a register of warrants that specifies the following particulars:

- Date the warrant was issued.
- Name of judge or 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.
- Any variation or extension of the warrant.

The VI identified incorrect dates recorded in the register for 2 inspected warrants.

Finding 2 – Incorrect dates recorded in the register of warrants.

DELWP is required to record in the register, amongst other things, the period that each warrant was in force. In one (1) inspected file, the revocation instrument gave the date of revocation as 3 May 2019. The register, however, recorded the same warrant was revoked on 5 May 2019. In another inspected file, although the warrant was endorsed with a new expiry date of 17 March 2019, the register showed that the same warrant was extended until 16 March 2019.

In response to the above-mentioned errors, DELWP corrected the register at the time of inspection.

FINDINGS – REPORTS

Were reports to the magistrate or judge properly made?

Under s 30K of the SD Act, 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. These reports 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 DELWP for the inspected warrants were made within the requisite timeframe, however 2 reports were identified with one (1) or more errors.

Finding 3 – Incorrect information given in the report to the judge/magistrate.

In one (1) inspected file the register recorded 5 search warrant applications as a general use of information obtained by use of the surveillance devices under the warrant however this use was not recorded in the report made to a justice of the Supreme Court of Victoria. For the same warrant, the end date given for use of surveillance devices in the report by the Technical Surveillance Unit (TSU) was found to not correlate with the date recorded in the report to the justice.

In one (1) other inspected warrant file, the report by the TSU and the report made to the magistrate contained different end dates for the use of surveillance devices.

DELWP advised that the above-mentioned anomalies were the result of incorrect information given in the reports made under s 30K of the SD Act, and confirmed it would make supplementary reports to correct these errors.

Was the annual report to the Minister properly made?

The VI found that DELWP was compliant with the reporting requirements of s 30L of the SD Act. The annual report made by the Secretary for the 2018-2019 financial year met all reporting criteria and was submitted to the Minister (Attorney-General) by 30 September 2019.

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 files inspected during 1 July to 31 December 2019.

Were issues identified at previous inspections addressed?

There were no issues to be addressed from the previous VI inspection.

The VI notes that DELWP was responsive and transparent during the inspection process. Although some instances of non-compliance were identified from our recent inspection of DELWP records, no significant compliance issues were identified.

In response to issues raised by the VI about certain records, DELWP demonstrated an eagerness to accept advice given by the VI, for example around the making of supplementary reports, and quickly took remedial action. The VI looks forward to, and expects, DELWP to achieve improved compliance with the provisions of the SD Act in future inspections.

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 July and 31 December 2019.

The VI found the GMA made an annual report for the 2018-2019 financial year under s 30L of the SD Act that met all reporting criteria. This report however was not submitted to the Minister (Attorney-General) until end of February 2020, significantly outside the specified timeframe of 30 September 2019. The VI acknowledges that the GMA's delay in making this report was likely the result of having misunderstood that a report is necessary even where it is a nil return. The GMA notified the VI that it has now added this requirement to its processes and the VI expects the GMA to fully comply with this reporting obligation in the future.

Independent Broad-based Anti-corruption Commission

The Independent Broad-based Anti-corruption Commission (IBAC)'s 'Legal Compliance Unit' administers surveillance device warrants issued to IBAC. The VI inspected 4 surveillance device files at IBAC on 13 November 2019, which constituted all relevant records associated with warrants that ceased between 1 January and 30 June 2019.

FINDINGS – WARRANTS

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

The VI found that the 4 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 a Supreme Court judge or magistrate, as appropriate.

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).

Three surveillance device warrants were issued, all of which were found to have met the above-mentioned requirements. One (1) application made by IBAC for a surveillance device warrant was refused.

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.

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

The VI found that IBAC kept a register of warrants, as required by s 300(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.
- Any variation or extension of the warrant.

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 to the magistrate or judge 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 3 reports made by IBAC for warrants that ceased between 1 January and 30 June 2019 were made within the requisite timeframe and complied with the above-mentioned requirements under ss 30K(1)-(2) of the SD Act.

Was the annual report to the Minister properly made?

The VI found that IBAC was compliant with the reporting requirements of s 30L of the SD Act. The annual report made by the Commissioner for the 2018-2019 financial year met all reporting criteria and was submitted to the Attorney-General by 30 September 2019.

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 July to 31 December 2019.

Were issues identified at previous inspections addressed?

Since no issues with IBAC files were identified from the VI's previous inspection of surveillance device records, there were no historical issues to be addressed on this occasion.



Victorian Fisheries Authority

Although 2 surveillance device warrants issued to the Victorian Fisheries Authority (VFA) ceased between 1 January and 30 June 2019, the VI inspected these files during the previous inspection period. The findings from the inspection of these files have consequently already been reported on. Since no other surveillance device warrants issued to the VFA ceased during the period covered by this report, the VI did not inspect any VFA files between 1 July and 31 December 2019.

In this report, the VI's assessment of the VFA's extent of compliance is limited to whether the reporting requirements of s 30L of the SD Act were met. The VI found that the annual report made by the CEO for the 2018-2019 financial year met all reporting criteria and was submitted to the Attorney-General by 30 September 2019.

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), 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 21 November 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) variation to an issued warrant) and 1 retrieval warrant, all of which ceased between 1 January and 30 June 2019. No emergency authorisations were made during this period. There were 2 surveillance device files at the TPU inspected on 9 October 2019, and 43 files at the SPU inspected from 19-20 November 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 a Supreme Court judge or magistrate, as appropriate.

In addition to meeting the above-mentioned requirements, the one (1) application to vary a warrant was correctly made to a magistrate in this instance.

Were warrants, including retrieval 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.

The one (1) issued retrieval warrant complied with s 20F of the SD Act by specifying the following:

- The name of the applicant and date warrant was issued.
- Kind of surveillance device authorised for retrieval and premises or object from which it is to be retrieved.
- Duration for the warrant (up to 90 days).
- Name of primary law enforcement officer responsible for executing the warrant.
- Any conditions for entry of premises.
- 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).

Victoria Police discontinued use of 37 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 did not make any emergency authorisations for the use of a surveillance device in the period.

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, with the exception of how the use made of information obtained by a surveillance device was recorded for one (1) issued warrant. Victoria Police confirmed that its electronic register had incorrectly omitted “brief of evidence” as a use of information obtained by a surveillance device. In response to our post-inspection feedback, Victoria Police notified that the register would be corrected; the VI will re-inspect this warrant file at the next scheduled inspection.

Victoria Police kept details on the destruction of records and reports related to 64 surveillance device warrants in accordance with s 30N(f) of the SD Act.

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.
- Any variation or extension of the warrant.

Since Victoria Police 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 to the magistrate or judge 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 in accordance with s 30K of the SD Act for warrants that ceased between 1 January and 30 June 2019 were made within the requisite timeframe, however 2 reports were identified with an error.

Finding 1 – Incorrect information given in the report to the judge/magistrate.

In the electronic register for one (1) warrant file “managing covert aspects of the investigation” was recorded as a use of information obtained by the surveillance device, yet the report made to the judge did not mention this as a use of the information obtained.

In one (1) other file, the end date for use of a surveillance device recorded in the report to the magistrate did not correlate with the date given in the report by the Technical Surveillance Unit (TSU) for the same device.

Victoria Police confirmed the discrepancies were caused by errors made in the reports to the magistrate and judge, and further advised that supplementary reports would be made under s 30K of the SD Act to correct these inaccuracies. The VI will re-inspect these warrant files at the next scheduled inspection.

Was the annual report to the Minister properly made?

The VI found that Victoria Police was compliant with the reporting requirements of s 30L of the SD Act. The annual report made by the Chief Commissioner for the 2018-2019 financial year met all reporting criteria and was submitted to the Attorney-General by 30 September 2019.

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?

Since no issues with Victoria Police files were identified from the VI's previous inspection of surveillance device records, there were no historical issues to be addressed on this occasion.

