



VICTORIAN INSPECTORATE

**Report of the Victorian Inspectorate to the Parliament of
Victoria in respect of the Department of Primary Industries
Pursuant to the *Surveillance Devices Act 1999***

Report No. 2 of 2012 - 2013

11 OCTOBER 2013

Table of Contents

INTRODUCTION	5
KEY PROVISIONS OF THE SD ACT	6
BACKGROUND FOR THE CURRENT LEGISLATION	6
PURPOSES OF THE SD ACT	6
STATE AGENCIES PERMITTED TO USE SURVEILLANCE DEVICES	6
TYPES OF SURVEILLANCE DEVICES	7
WARRANTS	7
<i>Surveillance Device Warrants</i>	7
<i>Retrieval Warrants</i>	8
REVOCATION	8
EXERCISE OF POWERS	8
RECENT CHANGES	8
THE ROLE OF THE VICTORIAN INSPECTORATE	9
THE POWERS OF THE VI UNDER THE SD ACT	9
INSPECTION METHODOLOGY	10
INTRODUCTION	10
INSPECTION OF WARRANT FILES AND OTHER RECORDS	10
UNDERSTANDING ‘PROTECTED INFORMATION’	10
DEFINING COMPLIANCE	11
INSPECTION RESULTS	12
INTRODUCTION	12
KEEPING DOCUMENTS CONNECTED WITH WARRANTS: SECTION 30M	12
<i>Documents to be kept under s. 30M – each warrant</i>	13
OTHER RECORDS TO BE KEPT: SECTION 30N	14
OTHER COMPLIANCE REQUIREMENTS	14
<i>Reports under s. 30K</i>	16
RECOMMENDATIONS	17
<i>Previous Recommendation</i>	17
<i>New recommendations</i>	17
INSPECTION SUMMARY	17
NEXT REPORT	18

List of Abbreviations

DEPI	Department of Environment and Primary Industries
DPI	Department of Primary Industries
DSE	Department of Sustainability and Environment
PI	Protected Information
PIM	Public Interest Monitor
SD Act	<i>Surveillance Devices Act 1999 (Vic)</i>
SIM	Special Investigations Monitor
VI	Victorian Inspectorate

INTRODUCTION

The *Surveillance Devices Act 1999* (Vic) (the SD Act) regulates the use of surveillance devices in the State of Victoria. The Act makes provision for warrants and emergency authorisations¹ permitting the installation, use, maintenance and recovery of surveillance devices by four State law enforcement agencies.² Use of surveillance devices in relation to private activity and private conversation is otherwise generally unlawful in Victoria.³

The SD Act imposes a regime of strict controls relating to the use of surveillance devices, including a requirement for agencies to make and keep records and documents and to destroy certain material when it is not likely to be further required for an authorised purpose. It also provides for independent inspection of agency records and documents by an independent officer who is responsible directly to the Victorian Parliament. From 1 July 2006 to 9 February 2013 the inspection function was the responsibility of the Special Investigations Monitor (SIM), a statutory officer whose responsibilities included inspecting agency records, assessing statutory compliance with the SD Act and reporting to the Parliament.

As discussed in the Victorian Inspectorate's (VI) previous report⁴ on 10 February 2013 the functions previously performed by the SIM were transferred, with minor modifications, to the newly established VI.

As with the VI's previous 'mid-year' report (which covered the first half of the 2012-2013 year),⁵ this second and final report for 2012-2013 is submitted to the Parliament of Victoria, with a copy provided to the Minister responsible for the SD Act (the Attorney-General) in accordance with the VI's obligation under s. 30Q. In previous years a single report covering the inspections of the four authorised State law enforcement agencies was prepared and submitted to the Parliament. For the second report of 2012-2013, individual reports for each agency have been prepared. This report details the results of inspections of the Department of Primary Industries (DPI) records conducted between 1 July 2012 and 30 June 2013 and other matters considered by the VI to be relevant to compliance with the SD Act by that agency.

¹ Emergency authorisations may be obtained by Victoria Police, the Independent Broad-based Anti-corruption Commission and the Australian Crime Commission only. Section 25 of the *Surveillance Devices Act 1999* (SD Act) expressly states that Emergency Authorisations are not available to the Department of Primary Industries (DPI) or law enforcement officers of the DPI.

² The Act also permits the Australian Crime Commission (ACC) to use the provisions of the SD Act. Inspection of resulting ACC records and documents is conducted by the Commonwealth Ombudsman pursuant to s 55(2) of the *Surveillance Devices Act 2004* (Cth).

³ The Act provides for certain exceptions at ss 5, 6(2), 7(2), 8(2), 9(2), 9B(2)(b) and (c), 9C(2).

⁴ Report of the Victorian Inspectorate pursuant to the *Surveillance Devices Act 1999* – Report No. 1 of 2012-2013.

⁵ *Ibid.*

KEY PROVISIONS OF THE SD ACT

Background for the current legislation

Background to the SD Act was set out in the SIM's 'Report of the Special Investigations Monitor to the Parliament of Victoria Pursuant to the *Surveillance Devices Act 1999* - Report No. 2 of 2008-2009' (dated 30 September 2009). This report, and all other SIM reports made in accordance with the SD Act, is now available on the VI's website.⁶

Purposes of the SD Act

The purposes of the SD Act include:⁷

- the regulation of the installation, use, maintenance and retrieval of surveillance devices
- the establishment of procedures for law enforcement officers to obtain warrants or emergency authorisations for the installation, use, maintenance and retrieval of surveillance devices
- the imposition of requirements for the secure storage and destruction of records and for the making of reports to judges, magistrates and the Parliament in connection with surveillance device operations
- the recognition (subject to the *Surveillance Devices Regulations 2006*) of warrants and emergency authorisations issued in another jurisdiction authorising the installation and use of surveillance devices.

State agencies permitted to use surveillance devices

- Victoria Police
- Office of Police Integrity – to 9 February 2013
- Independent Broad-based Anti-Corruption Commission – from 10 February 2013
- Department of Primary Industries
- Department of Sustainability and Environment

⁶ At <http://www.vicinspectorate.vic.gov.au>.

⁷ SD Act s 1.

Types of surveillance devices

The SD Act allows for the use of the following surveillance devices:

- data surveillance devices
- listening devices
- optical devices
- tracking devices.

Subject to obtaining appropriate authorisation, the use of devices for multiple functions is permitted.

Warrants

SURVEILLANCE DEVICE WARRANTS

The SD Act provides at s. 15(1) that a law enforcement officer may apply for the issue of a surveillance device warrant if the officer on reasonable grounds suspects or believes that:

- an offence has been, is being, is about to be or is likely to be committed; and
- use of a surveillance device is or will be necessary for the purpose of an investigation into that offence or of enabling evidence or information to be obtained of the commission of that offence or the identity or location of the offender.

The justification for use of surveillance devices for the purpose of furthering investigations depends very much on the nature and circumstances of each case and evaluating whether the use of devices might be expected to further the investigation.

An application may be made only with the approval of either a senior officer of the agency⁸ or an authorised police officer (being a person appointed by the Chief Commissioner of Police).⁹

Section 15(3) of the SD Act provides that an application for a surveillance device warrant may be made only to a judge of the Supreme Court of Victoria, except in the case of a tracking device, in which case the application may be made to a magistrate. There is provision for a 'remote application', that is, an application made by telephone, fax, email or

⁸ Defined in SD Act s 3(1).

⁹ Ibid ss 3(1) and 3(2).

other means of communication, in circumstances where it is impractical for an application to be made in person.¹⁰

RETRIEVAL WARRANTS

There is provision in the SD Act for issue of a retrieval warrant to authorise the recovery of a surveillance device where the device was lawfully installed on premises, or in or on an object under a surveillance device warrant. A surveillance device warrant authorises installation and retrieval within the period of the warrant. Therefore, a retrieval warrant is usually necessary only when a device was not retrieved before the warrant ceased to be in effect and retrieval without the authority of a warrant might constitute a trespass or other offence. Sections 20C to 20H of the SD Act govern the procedure for application, issue and revocation of retrieval warrants, with s. 20G detailing what is authorised by such a warrant.

Revocation

The provisions of the SD Act include a requirement for an agency chief officer to revoke a surveillance device warrant when the need for use of devices authorised by the warrant to obtain evidence of the commission of an offence, or to establish the identity or location of an offender, no longer exists. There is a similar provision requiring revocation of a retrieval warrant if the grounds for the application for the warrant cease to exist during the period of the warrant.

Exercise of Powers

Certain powers under the SD Act may be exercised by either senior officers of the agency concerned or authorised police officers.¹¹ For the DPI, 'senior officer' is defined as meaning the Secretary of the Department, who is therefore the only person within the DPI who may exercise those powers.

Recent changes

As noted earlier in this report, and in the VI's previous report,¹² the VI took over the inspection and reporting obligations of the SIM on 10 February 2013. On that date,

¹⁰ Ibid s 16.

¹¹ For example, see SD Act ss 15(2) and 20C(2).

¹² Above n 4.

amendments to the SD Act¹³ came into effect which introduced the Public Interest Monitor (PIM) into the process for making applications for surveillance device and retrieval warrants under the SD Act and placed additional notification and reporting obligations on law enforcement agencies in respect of the PIM.

On 1 July 2013, the DPI and Department of Sustainability and Environment (DSE) merged to form the Department of Environment and Primary Industries (DEPI). For this reason, while this report concerns the compliance of the DPI (as it was), any comment or recommendations are directed to the new DEPI.

The role of the Victorian Inspectorate

The VI is required by s. 30P of the SD Act to inspect the records of Victorian law enforcement agencies using surveillance devices under a warrant or emergency authorisation in order to determine the level of statutory compliance with the Act by the agency and its law enforcement officers.

The SD Act requires that inspections by the VI be carried out ‘from time to time’¹⁴ and that the VI report at six-monthly intervals to the Parliament as soon as practicable after 1 January and 1 July of each year. The VI is also required to provide a copy of each report to the Minister (Attorney-General).

The powers of the VI under the SD Act

For the purpose of an inspection under s. 30P the VI:¹⁵

- after notifying the chief officer of the agency, may enter at any reasonable time the premises occupied by the agency
- is entitled to have full and free access at all reasonable times to all records of the agency that are relevant to the inspection
- may require a member of staff of the agency to give any information that the VI considers necessary, being information that is in the member’s possession, or to which the member has access, and is relevant to the inspection.

¹³ Amendments made by Part 6 of the *Public Interest Monitor Act 2011*.

¹⁴ SD Act s 30P(1).

¹⁵ Ibid s 30P(2).

INSPECTION METHODOLOGY

Introduction

This report addresses the results of inspections undertaken of DPI and records the level of compliance with the SD Act, as assessed by the VI. The VI continues the practice adopted by the SIM by conducting two inspections of DPI records each financial year. Although the statutory requirement is for inspections to be conducted ‘from time to time’, the VI is required to report to Parliament every six months making it necessary that inspections occur at least bi-annually.

Inspection of warrant files and other records

Inspections of DPI records by the SIM since that agency assumed responsibilities under the SD Act in 2006 were conducted such that all available records were subject to inspection. This included records relating to warrants which were still in force and those warrants which had recently ceased to be force but for which the Report to the issuing judge or magistrate had not yet been completed. This methodology is different from that employed in respect of Victoria Police and the Office of Police Integrity (and subsequently the Independent Broad-based Anti-Corruption Commission) where a warrant file was inspected only after all statutory reporting requirements referable to that warrant had been completed and arose primarily due to the significant difference in the number of warrants being sought and issued to each agency and the complexity of inspecting records for a significant number of extant warrants which had to be reinspected at a later date after all administrative matters, (e.g. reporting pursuant to s.30K of the Act to the judge or magistrate who issued the warrant), had been completed. The VI has adopted the SIM’s methodology for inspecting files across all relevant agencies.

Understanding ‘protected information’

Before reporting inspection results, it is useful to note that under the SD Act ‘protected information’ (PI) includes:¹⁶

- information obtained through use of devices authorised by a warrant or an emergency authorisation
- information about an application for a warrant or emergency authorisation, made by a law enforcement officer

¹⁶ Ibid s 30D.

- information about a warrant issued (including a retrieval warrant), or an emergency authorisation granted by a ‘senior officer’ (within the meaning of the Act) of the agency
- information about an application to a judge for approval of the use of emergency powers.

SD Act provisions limit the use, communication or publication of PI,¹⁷ including both ‘local PI’¹⁸ and ‘corresponding PI’.¹⁹ In summary:

- ‘local PI’ means information obtained from or relating to a warrant or emergency authorisation issued under the SD Act²⁰
- ‘corresponding PI’ means information obtained from or relating to a warrant or emergency authorisation issued under a ‘corresponding law’²¹ of another jurisdiction.²²

The SD Act requires that records or reports obtained by use of a surveillance device are kept secure and are not accessible to unauthorised persons.²³ Such records and reports fall within the definition of PI. Further, because there are statutory restrictions on the use, communication and publication of PI, the practical effect is that an agency must keep all PI secure; not only the reports and records obtained by the use of a surveillance device, but also associated information and documents connected with the warrant or emergency authorisation.

For the purpose of this report, the term ‘PI’ is used when referring to information obtained by means of a surveillance device, although as noted above its statutory definition is much wider.

Defining compliance

Three categories are used in this report to describe the level of statutory compliance.

Compliant – the agency was either fully compliant, or any degree of non-compliance was relatively trivial and in the nature of an occasional mistake or an oversight.

¹⁷ Ibid s 30E.

¹⁸ Ibid s 30F.

¹⁹ Ibid s 30G.

²⁰ Ibid s 30F(4).

²¹ Defined in SD Act s 3.

²² Ibid s 30G(4).

²³ Ibid 30H.

Substantially Compliant – the agency had appropriate forms and procedures in place to meet compliance requirements, but there was a compliance problem, for example, with the forms or with the content of completed documents and records, or with procedures.

Not Compliant – a substantial or complete failure to comply with statutory requirements.

INSPECTION RESULTS

Introduction

In 2012-2013, the DPI sought and obtained three surveillance device warrants. Two of these were inspected in the first half of this year and the results of that inspection were discussed in general terms in the VI's last report.²⁴ The third warrant was issued in the days immediately prior to the second VI inspection of DPI records and had not yet been executed at the time of that inspection. Each of these warrants was obtained in connection with the investigation of suspected offences under the *Fisheries Act 1995*. This report provides detail of the results of the second inspection for the year and a summary of the compliance performance over the full year.

Tables 1 to 3 below summarise statutory compliance requirements relevant to the VI's inspection of DPI records and documents concerning the three warrants. The tables also record whether or not compliance was achieved by the agency in each of those categories. When appropriate, additional comment is made in the body of the report.

Certain compliance requirements are marked in the tables as not assessed (N/A) because those requirements do not apply in relation to the warrant records inspected.

Keeping documents connected with warrants: Section 30M

Section 30M of the SD Act provides that the Secretary of the DPI, as chief officer of the agency, must cause certain surveillance device warrant documents to be kept in the records of the agency.

A summary of the level of compliance achieved by the DPI with s. 30M is set out in Table 1 below. To the extent relevant, the agency was compliant with s. 30M of the SD Act.

²⁴ Above n 4.

TABLE 1: COMPLIANCE WITH THE SD ACT - DOCUMENTS TO BE KEPT: S. 30M

Documents to be kept under s30M	Level of Compliance	Comment
Each warrant. s. 30M(a)	Compliant	See comments below.
Each notice of revocation by a judge or magistrate under s. 20A(3). s. 30M(b)	N/A	No warrants revoked under s. 20A.
A copy of each application for a warrant, extension, variation or revocation of a warrant. s. 30M(e)	Compliant	All warrant applications were held. The other documents were not relevant.
A copy of each report to a judge or magistrate under s. 30K. s. 30M(f)	Compliant	
A copy of each evidential certificate issued under s. 36. s. 30M(g)	N/A	No data used evidentially to date of inspection.

DOCUMENTS TO BE KEPT UNDER S. 30M – EACH WARRANT.

In the previous VI report²⁵ it was noted that the two warrants issued in the period under report were deficient when issued in that neither specified a time within which a report to the issuing magistrate was required to be made under s. 30K of the SD Act. The specification of such a time is a requirement of s. 18(1)(b)(xi) of the SD Act. That report also noted that once this omission had been detected by DPI staff, an application was made to the issuing magistrate for a report time to be set and such a date was consequently nominated and the warrant amended by way of a signed endorsement made by the magistrate.

The DPI staff advised during the first inspection of records that this omission would lead to the revision of the template used by the agency for the purpose of preparing a warrant to ensure it includes a provision to state the date by which a report must be made. It was evident during the second inspection of DPI records that the template had been revised. The warrant issued immediately prior to the inspection included a paragraph which provided for the issuing magistrate to state the date by which a report under s. 30K was to be made.

²⁵ Above n 4.

Other records to be kept: Section 30N

Section 30N of the SD Act provides that the Secretary of the DPI must cause certain records in connection with surveillance devices to be kept in the records of the agency. A summary of the level of compliance achieved by the DPI with s. 30N is set out in Table 2 below.

The VI considers that compliance was achieved with s 30N(a) and (c) which, as Table 2 demonstrates, were the only subsections applicable in the year under report to the warrants obtained by the DPI.

TABLE 2: COMPLIANCE WITH THE SD ACT - RECORDS TO BE KEPT: S. 30N

Records to be kept under s30N	Level of Compliance	Comment
Statement as to whether each application for a warrant, extension, variation or revocation was granted, refused or withdrawn. s. 30N(a)	Compliant	
Details of each use of information obtained by use of an SD under a warrant. s. 30N(c)	Compliant	
Details of each communication to a person other than a law enforcement officer of the agency, of information obtained by the use of an SD. s. 30N(d)	N/A	No external communications of PI occurred.
Details of each occasion when, to the knowledge of a law enforcement officer of the agency, information obtained by an SD was given in evidence in a 'relevant' proceeding. s. 30N(e)	N/A	Investigation ongoing. No evidential use of PI.
Details of the destruction of records or reports under s. 30H(1)(b). s. 30N(f)	N/A	None undertaken.

Other compliance requirements

Additional to the requirement to keep certain documents and records, the Secretary of the DPI is required to comply with a number of other obligations imposed by the SD Act. These include:

- causing a register of warrants to be kept, in compliance with s. 30O
- ensuring the use of a device is discontinued and the warrant is revoked, in compliance with s. 20B(2) and (3)
- revocation of a retrieval warrant, in compliance with s. 20H

- ensuring every record or report obtained by use of a device under the SD Act is secure from unauthorised access, in compliance with s. 30H(1)(a)
- destroying or causing any record to be destroyed, in compliance with s. 30H(1)(b), when satisfied it is not likely to be required for a purpose referred to in s. 30E(4), 30F(1) or 30G(1) of the SD Act
- submitting an annual report to the Minister covering information prescribed in s. 30L of the SD Act.

Law enforcement officers to whom a warrant is issued, or who are primarily responsible for the execution of a warrant, also have particular compliance responsibilities, namely:

- to immediately inform the Secretary of the DPI if he/she believes -
 - the use of a device under an SD warrant is no longer necessary for obtaining evidence of the commission of an offence or to establish the identity or location of the offender,²⁶ or
 - grounds for issue of a retrieval warrant no longer exist (usually once the device(s) has been recovered);²⁷ and
- to make a report in accordance with s. 30K to the judge or magistrate who issued the warrant, within the time specified in the warrant.

Two general compliance requirements of the SD Act are required of the DPI, namely:

- an application for a warrant may be made only with the approval of a ‘senior officer’²⁸
- an application for a retrieval warrant may be made only with the approval of a ‘senior officer’.²⁹

A summary of the level of compliance achieved by the DPI with all of these provisions is set out in Table 3 below.

²⁶ SD Act s 20B(4).

²⁷ Ibid s 20H(4).

²⁸ Ibid s 15(2).

²⁹ Ibid s 20C(2).

TABLE 3: COMPLIANCE WITH THE SD ACT – OTHER REQUIREMENTS

Other Compliance Requirements	Level of Compliance	Comment
Maintain a register of warrants and emergency authorisations with required details. s. 30O	Compliant	
Discontinue use of SD and revoke SD warrant in certain circumstances. s. 20B	N/A	
Revocation of retrieval warrants by chief officer. s. 20H(3)	N/A	No retrieval warrants had been obtained or sought.
Records and reports obtained by use of an SD under warrant kept secure from unauthorised persons. s. 30H(1)(a)	Compliant	
Destruction of records and reports. s. 30H(1)(b)	N/A	None undertaken.
Annual report to Minister by chief officer of the agency. s. 30L	Compliant	The report was made by the date required.
Law enforcement officer to inform chief officer if use of SD no longer necessary or grounds for retrieval warrant cease to exist. s. 20B(4) & s. 20H(4)	N/A	
Report to judge or magistrate under s. 30K made on time and includes required information. s. 30K(1)	Substantially compliant	Error in information reported.
Applications made only with the approval of a 'senior' or 'authorised' officer. s. 15(2)	Compliant	

REPORTS UNDER S. 30K

Several significant errors were detected in the reports on the two warrants inspected in the first half of the year and for which reports had been made pursuant to s. 30K of the SD Act. These errors concerned incorrect information in reporting the names of persons involved in the execution of the respective warrants and the periods during which the SDs were used. The reports were otherwise compliant and were made before the date due.

Recommendations

PREVIOUS RECOMMENDATION

The SIM made one recommendation the second report of the 2011-2012 year, being that the DPI should obtain receipts when delivering reports made pursuant to s. 30K of the SD Act, or that some other record of transmittal of the report be made by the DPI officer delivering the report.

In response to the draft of that report, the Secretary of the DPI advised the VI that the recommendation would be implemented. Subsequent inspection of the DPI records revealed this recommendation had been implemented and records inspected provided clear information as to the date on which reports under s. 30K of the SD Act were provided to the issuing magistrate.

NEW RECOMMENDATIONS

No new recommendations are made.

Inspection summary

While the DPI has developed compliant document templates and procedures, with the agency utilising the provisions of the SD Act infrequently, error or omission in the records for a very small number of SD warrants has a significant impact on the assessment of compliance with the Act. Notwithstanding this hurdle, the VI is able to report that the DPI was compliant during the 2012-2013 inspection with all statutory requirements except for errors found in reports to a judge or magistrate. Such a report is required by s. 30K of the SD Act which details the matters to be included in each report. While the required content was included in the DPI reports some of the information provided was inaccurate.

The VI records his appreciation for the full cooperation and assistance accorded to his staff in the inspection of agency records.

NEXT REPORT

As required by s. 30Q of the SD Act, the VI will next report as soon as practicable after 1 January 2014. Due to the merging of the former DSE and DPI from 1 July 2013, the next inspection and report will be in relation to the use of SDs by the new DEPI.

A handwritten signature in blue ink that reads "Robin Brett". The signature is written in a cursive style and is placed on a light-colored, slightly textured rectangular background.

Robin Brett QC
Inspector
Victorian Inspectorate