Report of the Victorian Inspectorate to the Parliament of Victoria in respect of the Independent Broad-based Anti-corruption Commission Pursuant to the *Surveillance Devices Act 1999*

Report No. 2 of 2012 - 2013

11 OCTOBER 2013

Table of Contents

List of Abbreviations

IBAC	Independent Broad-based Anti-corruption Commission
OPI	Office of Police Integrity
PI	Protected Information
PIM	Public Interest Monitor
SD Act	*Surveillance Devices Act 1999* (Vic)
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 authorisations permitting the installation, use, maintenance and recovery of surveillance devices by four State law enforcement agencies.[1] Use of surveillance devices in relation to private activity and private conversation is otherwise generally unlawful in Victoria.[2]

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 report,[3] on 10 February 2013 the functions previously performed by the SIM were transferred, with minor modifications, to the newly established VI. At the same time, the Office of Police Integrity (OPI) was abolished and the Independent Broad-based Anti-corruption Commission (IBAC) was created. The IBAC took possession or control of all information, documents, reports and records then in the possession or control of OPI immediately before the relevant legislation[4] came into force on 10 February 2013. The data transferred included records pertaining to all warrants and authorisations issued to OPI under the SD Act.

---

[1] The *Surveillance Devices Act 1999* (SD 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).

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

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

[4] *Independent Broad-based Anti-corruption Commission Amendment (Investigative Functions) Act 2012*.

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 includes the results of inspections of OPI 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.

KEY PROVISIONS OF THE SD ACT

Background to 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 are now available on the VI's webpage.[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

[5] Above n 3.
[6] At http://www.vicinspectorate.vic.gov.au.
[7] SD Act s 1.

- 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.

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

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 and emergency authorisations

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 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 agency,[8] 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 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 governs the procedure for application, issue and revocation of retrieval warrants, with s. 20G detailing what is authorised by such a warrant.

[8] Defined in SD Act s 3(1).
[9] Ibid ss 3(1) and 3(2).
[10] Ibid s 16.

EMERGENCY AUTHORISATIONS

The SD Act makes provision for an emergency authorisation to be granted by a 'senior officer' for use of surveillance devices, where there is an imminent threat of serious violence to a person or of substantial damage to property[11] or where the intended use of a device relates to a serious drug offence.[12] These emergency authorisation provisions may be used only where the seriousness and urgency of the situation justify the use of a surveillance device and it is not practicable in the circumstances to apply for a warrant. Emergency authorisation may be given only if the senior officer is satisfied that there are reasonable grounds for the officer's suspicion or belief founding the application.

Where emergency authorisation is granted, a senior officer (or another person acting on his or her behalf) must apply within two business days to a Supreme Court judge for approval of the exercise of powers under that authorisation.[13] Emergency authorisations are available only to Victoria Police and IBAC.[14]

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 before the warrant expires. Typically, revocation of a retrieval warrant is necessary once the retrieval of any SDs under the authority of the warrant has occurred.

[11] Ibid s 26.
[12] Ibid s 27.
[13] Ibid s. 28(1)
[14] Section 25 specifically excludes the Department of Primary Industries and the Department of Sustainability and Environment from the emergency authorisation provisions. Emergency authorisation provisions were also available to OPI.

Exercise of powers

Certain powers under the SD Act may be exercised by either senior officers of the agency concerned or authorised police officers.[15]

The definition of 'senior officer' as it relates to IBAC, is defined in r. 3 of the SD Regulations as the positions of IBAC Deputy Commissioner and Chief Executive Officer and also IBAC Officers classified as Executive Officers.

Recent changes

As noted earlier in this report and in the VI's previous report,[16] the VI took over the inspecting and reporting obligations of the SIM on 10 February 2013. On that date, amendments to the SD Act[17] 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.

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'[18] 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).

[15] For example, see SD Act ss 15(2) and 20C(2).
[16] Above n 3.
[17] Amendments made by Part 6 of the *Public Interest Monitor Act 2011*.
[18] SD Act s 30P(1).

The powers of the VI under the SD Act

For the purpose of an inspection under s. 30P the VI:[19]

- 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.

INSPECTION METHODOLOGY

Introduction

This report addresses the results of inspections undertaken of OPI and IBAC and records the level of compliance with the SD Act, as assessed by the VI. While the statutory requirement for inspection of agency records is that they 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. To that end, the VI continued the methodology adopted by the SIM of inspecting OPI and IBAC records twice each year.

Inspection of warrant files and other records

The VI has continued to inspect OPI (and IBAC) warrant files on the basis detailed in the SIM's first report for 2009-2010.[20] Accordingly, a warrant file was inspected only after all statutory reporting requirements referable to that warrant had been completed. Such reporting was invariably completed within three months of the warrant ceasing to be in effect. This method worked well and negated the need to return to warrant files to address matters not finalised at the time of an inspection. All warrant files were inspected; to date, sampling has not been necessary. The result of this methodology is that the VI's report covers those warrants that ceased to be in force

[19] Ibid s 30P(2).

[20] Report of the Special Investigations Monitor to the Parliament of Victoria Pursuant to the *Surveillance Devices Act 1999* – Report No. 1 of 2009-2010.

during the most recently completed calendar year, in this case, the 2012 calendar year, and therefore, concerns only warrants issued to OPI (and not IBAC).

Understanding 'protected information'

Before reporting inspection results, it is useful to note that under the SD Act 'protected information' (PI) includes:[21]

- 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
- 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,[22] including both 'local PI'[23] and 'corresponding PI'.[24] In summary:

- 'local PI' means information obtained from or relating to a warrant or emergency authorisation issued under the SD Act[25]
- 'corresponding PI' means information obtained from or relating to a warrant or emergency authorisation issued under a 'corresponding law'[26] of another jurisdiction.[27]

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.[28] Such records and reports fall within the definition of PI. Further, because there are statutory restrictions

[21] SD Act s 30D.
[22] Ibid s 30E.
[23] Ibid s 30F.
[24] Ibid s 30G.
[25] Ibid s 30F(4).
[26] Defined in SD Act s 3.
[27] Ibid s 30G(4).
[28] Ibid s 30H.

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 to 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.

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.

Reconciling VI's data and Chief Officer annual reports.

This report makes reference to the number of warrant files inspected during the year. For the reasons outlined below, these numbers will not necessarily correlate with warrant numbers provided by agency chief officers in the reports made to the Minister and subsequently tabled in the Parliament pursuant to s. 30L of the SD Act.

Reports under s. 30L include statistical data concerning surveillance device warrants. That data covers warrants issued in the period 1 July to 30 June next. However, the VI's inspection of OPI warrant records did not include warrants still active at the time

of inspection or those for which reporting on expired warrants under s. 30K of the SD Act was not complete. Further, inspection of active PI registers by the VI can involve warrants which, because of the protracted nature of the investigation and/or of the court proceedings, may have already expired a year or more beforehand.

It is, therefore, not possible to reconcile statistics from s. 30L reports with those reported by the VI.

INSPECTION RESULTS

Introduction

The VI's previous report covering the first half of 2012-2013[29] stated that OPI had only three surveillance device warrants due for inspection. Each of these warrants was executed and all expired in March 2012. No retrieval warrants or emergency authorisations were sought or obtained by OPI in the 2012 calendar year, and no further surveillance device warrants were sought or obtained subsequent to the expiration of the warrants noted above. In effect, this means that there was one inspection of OPI warrant files and records in the year under report.

The VI still made an inspection visit to the IBAC in the second half of the year under report, notwithstanding there were no records to inspect. This was for the purpose of ascertaining the status of OPI information, documents, reports and records which passed into the possession of IBAC and for the security of which the IBAC became responsible on 10 February 2013.

The VI's previous report (referred to above) provided an interim report on inspection of OPI SD records in the first half of the 2012-2013 year. Following the practice of the SIM in recent years, this second report would have then provided a more comprehensive report covering the results of the second inspection for the year and summarising the compliance performance of the agency across the full year. In the circumstances of OPI ceasing to be an agency and the establishment of the IBAC

[29] Above n 3.

(which had no new SD records to inspect) this report must of necessity report on the compliance performance of OPI until its dis-establishment.

Keeping documents connected with warrants: Section 30M

Section 30M of the SD Act provided that as the chief officer of the agency, the Director, Police Integrity, must cause particular SD warrant documentation to be kept in the records of the agency.

A summary of the level of OPI compliance with s. 30M is set out in Table 1 below.

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	
Each notice of revocation by a judge or magistrate under s. 20A(3). s. 30M(b)	N/A	No revocations of this type occurred.
Each emergency authorisation. s. 30M(c)	N/A	No emergency authorities were granted or sought.
Each application for an emergency authorisation, warrant, extension, variation or revocation of a warrant, or for approval of the exercise of powers under an emergency authorisation. s. 30M(d) &(e)	Compliant	
A copy of each report to a judge or magistrate under s. 30K. s. 30M(f)	Compliant	
A copy of each certificate issued under s. 36. s. 30M(g)	Compliant	

Other records to be kept: Section 30N

Section 30N of the SD Act provided that the Director, Police Integrity must cause certain records to be kept in connection with surveillance devices.

A summary of the level of OPI compliance with s. 30N is set out in Table 2 below.

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

Records to be kept under s30N	Level of Compliance	Comment
A statement as to whether each application for a warrant, extension, variation or revocation was granted, refused or withdrawn. s. 30N(a)	Compliant	Recorded in the Register required to be kept under s. 30O.
A statement as to whether each application for an emergency authorisation or for approval of powers exercised under an emergency warrant, was granted, refused or withdrawn. s. 30N(b)	N/A	No emergency authorities were granted or sought.
Details of each use of information obtained by use of a 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 a SD. s. 30N(d)	Compliant	
Details of each occasion when, to the knowledge of a law enforcement officer of the agency, information obtained by a SD was given in evidence in a 'relevant' proceeding. s. 30N(e)	N/A	
Details of the destruction of records or reports under s. 30H(1)(b). s. 30N(f)	N/A	

Other compliance requirements

In addition to the requirement to keep certain documents and records, the Director, Police Integrity had a number of other compliance responsibilities. These included:

- causing a register of warrants to be kept in compliance with s. 30O of the SD Act
- ensuring that use of a device was discontinued when prescribed conditions existed and that the warrant was 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 was secure from unauthorised access, in compliance with s. 30H(1)(a)
- destroying or causing to be destroyed, any record or report obtained by use of a device 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, in compliance with s. 30H(1)(b)

- submitting an annual report to the Minister covering information prescribed in s. 30L of the SD Act.

Law enforcement officers to whom a warrant was issued, or who were primarily responsible for the execution of a warrant, also had particular compliance responsibilities, namely:

- to immediately inform the Director, Police Integrity if he/she believed:
  - the use of a device under a surveillance device warrant was no longer necessary for obtaining evidence of the commission of an offence or to establish the identity or location of an alleged offender, or
  - grounds for issue of a retrieval warrant no longer existed (usually once the device(s) had been recovered)
- 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 that:

- s. 15(2) provides that an application for a surveillance device warrant may be made only with the approval of a 'senior officer' (within the meaning of the SD Act)
- s. 20C(2) provides that an application for a retrieval warrant may be made only with the approval of a 'senior officer'.

A summary of the level of OPI compliance with these provisions is set out in Table 3 below, with further comment following the table.

REGISTER OF WARRANTS AND EMERGENCY AUTHORISATIONS: SECTION 30O

OPI kept an electronic register of warrants and emergency authorisations in satisfaction of s. 30O of the SD Act. The Register included all the requisite information, but the VI's Compliance Officers identified errors in respect of the data relating to the three warrants inspected.

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	Substantially compliant	See comments below
Discontinue use of SD and revoke SD warrant in certain circumstances. s. 20B	Compliant	
Revocation of retrieval warrants by chief officer. s. 20H(3)	N/A	No retrieval warrants in force in the period.
Records and reports obtained by use of a SD under warrant kept secure from unauthorised persons. s. 30H(1)(a)	Compliant	
Destruction of records and reports. s. 30H(1)(b)	Compliant	
Annual report to Minister by chief officer of the agency. s. 30L	Compliant	
Law enforcement officer to inform chief officer if use of SD no longer necessary or grounds for the warrant cease to exist. s. 20B(4) & s. 20H(4)	Compliant	
Report to judge or magistrate under s. 30K made on time and including required information. s. 30K(1)	Compliant	
Applications made only with the approval of a 'senior' or 'authorised' officer. s. 15(2)	Compliant	

Against each of the warrants inspected, the Register recorded incorrect dates in respect of:

- the date of issue of the warrant,
- the date of issue of extension of the warrant, and
- the date before which a report under s. 30K to the issuing magistrate was to be made.

The VI's Compliance Officers informed OPI of these errors, which were subsequently corrected.

While these errors can be categorised as mistakes rather than omissions, that the same errors attached to each of the warrants subject to inspection is of some concern. In

respect of compliance with s. 30O (to keep a register containing certain information) the VI has considers OPI to have been substantially compliant.

Security of data transferred to IBAC: s. 30H(1)

In receiving records and reports containing information obtained by means of an SD from OPI, the IBAC must comply with section 30H(1) of the SD Act and keep that information secure from persons not authorised to deal with it. The VI is satisfied from visiting the IBAC and from discussions with IBAC staff, that the material concerned remains as secure under IBAC control as it was under OPI. The VI therefore considers the IBAC to be compliant with s. 30H(1).

Inspection summary

The year under report was the final year of the OPI's operation and, as was the case in 2011-2012, OPI used the provisions of the SD Act sparingly.

The OPI was compliant with the requirements of the Act except in relation to a number of errors identified in the register kept pursuant to s. 30O.

OPI SD records were transferred to the IBAC in February 2013. From the VI's compliance inspection perspective they will be relevant in connection with the future destruction, in compliance with s. 30H(2), of former OPI records and of reports obtained by means of a surveillance device.

At the time of this report, IBAC has yet to make an application for a warrant or exercise the emergency authorisation provisions of the SD Act. The VI understands, the IBAC is in the process of devising policies and procedures in respect of surveillance device administration.

The IBAC is considered compliant with statutory requirements to secure SD information transferred to the IBAC from OPI and prevent access by unauthorised persons.

NEXT REPORT

As required by s. 30Q of the SD Act, the VI will next report on the results of inspection of IBAC records as soon as practicable after 1 January 2014.

Robin Brett QC
Inspector
Victorian Inspectorate.