Report of an audit of applications for and execution of surveillance device warrants limited to data surveillance, optical surveillance and tracking surveillance by the Independent Commission Against Corruption

by

The Inspector of the
Independent Commission Against Corruption

November 2009

CONTENTS

THE PURPOSE OF THE AUDIT

From time to time, as part of its investigations into alleged serious and systemic corrupt conduct, the Independent Commission Against Corruption (the ICAC or the Commission) obtains surveillance device warrants pursuant to the *Surveillance Devices Act 2007* (the SD Act).

During the course of conducting an audit of applications for and execution of listening device warrants by the Commission (the report of which was published in September 2009) it was apparent that in the one application warrants for the use of more than one class of surveillance warrant would be sought.

Accordingly, the present audit examines the Commission's applications for and execution of Surveillance Device Warrants limited to Data surveillance, Optical surveillance and Tracking surveillance.

Section 4 of the SD Act contains the following definitions:

"Surveillance device" means:

> (a) a data surveillance device, a listening device, an optical surveillance device or a tracking device, or
>
> (b) a device that is a combination of any 2 or more of the devices referred to in paragraph (a), or
>
> (c) a device of a kind prescribed by the regulations.

"Data surveillance device" means:

> any device or program capable of being used to record or monitor the input of information into or output of information from a computer, but does not include an optical surveillance device.

"Optical surveillance device" means:

> any device capable of being used to record visually or observe an activity, but does not include spectacles, contact lenses or a similar device used by a person with impaired sight to overcome that impairment.

"Tracking device" means:

> any electronic device capable of being used to determine or monitor the geographical location of a person or an object.

The use of such surveillance devices to monitor a person's computer and/or to observe and monitor a person's movements and to record such observations without the knowledge of that person is a serious intrusion into the right of privacy of that person.

In addition, such use is a covert activity the presence of which is an unknown to that person. Consequently, he/she is not in a position to raise a complaint or protest.

On the other hand, there are circumstances in which the covert use of surveillance devices can provide evidence which can facilitate the detection and/or prevention of a serious crime or aid the prosecution of a person or persons involved in serious criminal activity.

The SD Act after prohibiting the use of surveillance devices and the publication of the fruits of such use goes on to authorise the ICAC covertly to use data, optical and tracking surveillance devices in limited circumstances.

The purpose of this audit is to examine a sample of cases in which the ICAC has used such surveillance devices:

1. to determine whether it has obeyed the terms of the legislation.

2. to examine the systems instituted and maintained by the ICAC to ensure that such use is limited to those circumstances where it is lawful and appropriate for the conduct of its statutory functions.

3. to determine whether such use has in fact been appropriate to the conduct of its statutory functions.

This audit will cover the following:

1. The Inspector's audit function
2. The ambit of the audit
3. An anomaly in the legislation and suggested amendments
4. The relevant provisions of the SD Act
5. ICAC's systems to control and regulate the application for and use of surveillance device warrants
6. Truth of the contents of affidavits
7. Case studies
8. Conclusions

1 THE INSPECTOR'S AUDIT FUNCTION

Section 57B(1)(a) of the *Independent Commission Against Corruption Act 1988* (the ICAC Act or the Act) authorises the Inspector of the Independent Commission Against Corruption (the Inspector) to audit the operations of the ICAC for the purpose of monitoring compliance with the law of the State.

The Inspector's audit role must be read in the context of the Inspector's other functions prescribed under section 57B, namely section 57B(1)(c) and (d).

Section 57B(1)(c) of the ICAC Act authorises the Inspector to deal with (by reports and recommendations) conduct amounting to maladministration (including, without limitation, delay in the conduct of investigations and unreasonable invasions of privacy) by the Commission or officers of the Commission.

Section 57B(1)(d) of the ICAC Act authorises the Inspector to assess the effectiveness and appropriateness of the procedures of the Commission relating to the legality and propriety of its activities.

Section 57B(2) states that the functions of the Inspector may be exercised on the Inspector's own initiative.

2 THE AMBIT OF THE AUDIT

By letter dated 3 September 2009 I wrote to the Commissioner in the following terms, omitting formal parts:

> Pursuant to section 57B of the *Independent Commission Against Corruption Act 1988* (the Act), I propose to audit and assess the effectiveness and appropriateness of the procedures of the Commission in relation to the application for and execution of the Surveillance Device Warrants and Retrieval Warrants pursuant to Part 3 of the *Surveillance Devices Act 2007* (the SD Act) limited to Data Surveillance, Optical Surveillance and Tracking Surveillance devices.
>
> The proposed audit and assessment will examine:
>
> 1. the Commission's compliance with the formal and procedural requirements under the SD Act;
> 2. the reasons behind the Commission's decision to apply for such warrants;
> 3. the manner in which the Commission executed the warrants; and
> 4. any other matters set out in section 57B of the ICAC Act.
>
> For the purposes of this exercise I would, in the first instance, like to review the Commission's files and records relating to all applications for Surveillance Device Warrants and Retrieval Warrants pursuant to Part 3 of the SD Act limited to Data, Optical and Tracking Surveillance Devices during the period from 1 February 2009 to 30 June 2009, regardless of whether they were granted or refused by an eligible judge or magistrate.
>
> Upon reviewing the materials identified above I may request further information from the Commission and/or its officers for the purpose of completing my audit and assessment. I welcome any comments you

may have on the proposed ambit of this audit and assessment including any conditions you may require relating to the manner in which the information furnished to me will be dealt with.

The Commissioner replied by letter dated 29 May 2009 in the following terms, omitting formal parts:

> I refer to your letter dated 3 September 2009 advising that pursuant to section 57B of the ICAC Act you will conduct an audit and assessment of the effectiveness and appropriateness of the Commission's procedures in relation to the application for and execution of surveillance device warrants and retrieval warrants.
>
> You have requested files and records relating to all applications for surveillance device warrants and retrieval warrants, limited to data, optical and tracking devices, for the period 1 February 2009 to 30 June 2009.
>
> No information relating to any of these applications is currently in the public domain.
>
> The documentation comes within the definition of "protected information" as defined in section 39 of the *Surveillance Devices Act 2007* (the SD Act). The SD Act places limitations on the use of communication of "protected information". Section 40 of the Act makes it an offence to communicate or publish "protected information".
>
> Section 40(4) of the SD Act allows "protected information" to be published or communicated for the purpose of a "relevant proceeding". A "relevant proceeding" includes "an enquiry before the Inspector of the Independent Commission Against Corruption". The current audit and assessment would not appear to be "an enquiry before the Inspector of the Independent Commission Against Corruption".
>
> Section 40(6) of the SD Act provides that a chief officer may consent to the communication of protected information if satisfied that it is necessary or desirable in the public interest for the protected information to be communicated to the person concerned and that the public interest in communicating the information out ways any intrusion of the privacy of the person to whom it relates or of any other person who may be affected by its communication. Section 40(7) provides that in deciding whether to give consent the chief officer must take into consideration the manner in which the protected information will be dealt with after it is communicated to the person concerned.

I have determined that it is in the public interest to provide the relevant "protected information" to you and enclose a copy of the signed consent.

3 ANOMALY IN THE LEGISLATION AND SUGGESTED AMENDMENTS

The Commissioner contends (in my view correctly) that the provisions of the SD Act to which he refers, prima facie, prohibit him from furnishing "protected information" to the Inspector for the purpose of an audit (as opposed to the purpose of a targeted inquiry). In the present case, applying sections 40(6) and 40(7), he has determined that it is in the public interest to provide the information and has done so.

This means that the Inspector's power to conduct an audit of the use of any surveillance device is dependant upon the willingness of the Commissioner to make a determination that it is in the public interest to provide the information.

This is contrary the provisions of section 57C of the ICAC Act which sets out the Inspector's powers, namely:

> The Inspector:
>
> (a) may investigate any aspect of the Commission's operations or any conduct of officers of the Commission, and
>
> (b) is entitled to full access to the records of the Commission and to take or have copies made of any of them, and
>
> (c) may require officers of the Commission to supply information or produce documents or other things about any matter, or any class or kind of matters, relating to the Commission's operations or any conduct of officers of the Commission, and
>
> (d) may require officers of the Commission to attend before the Inspector to answer questions or produce documents or other

If the Inspector is to be able to exercise the duty of conducting audits in accordance with his powers, the SD Act should be amended by, for example, adding a subsection (8) to section 40 to the effect that nothing in this section shall be deemed to limit the powers of the Inspector under section 57C of the ICAC Act.

The records of the ICAC relating to listening devices are inspected by the Ombudsman pursuant to section 48 of the SD Act. However, the Ombudsman merely checks the accuracy of the records – not the appropriateness of the application for and use of the device.

4 THE RELEVANT PROVISIONS OF THE SURVEILLANCE DEVICES ACT

The relevant definitions in section 4 of the SD Act have been set out above.

Section 8 of the SD Act provides:

> (1) A person must not knowingly install, use or maintain an optical surveillance device on or within premises or a vehicle or on any other object, to record visually or observe the carrying on of an activity if the installation, use or maintenance of the device involves:
>
> (a) entry onto or into the premises or vehicle without the express or implied consent of the owner or occupier of the premises or vehicle, or
>
> (b) interference with the vehicle or other object without the express or implied consent of the person having lawful possession or lawful control of the vehicle or object.
>
> Maximum penalty: 500 penalty units (in the case of a corporation) or 100 penalty units or 5 years imprisonment, or both (in any other case).

This prohibition does not apply to the installation, use or maintenance of an optical surveillance device in accordance with a warrant, emergency authorisation, corresponding warrant or corresponding emergency authorisation.

Section 9 of the SD Act provides:

> (1) A person must not knowingly install, use or maintain a tracking device to determine the geographical location of:
>
> (a) a person—without the express or implied consent of that person, or
>
> (b) an object—without the express or implied consent of a person in lawful possession or having lawful control of that object.
>
> Maximum penalty: 500 penalty units (in the case of a corporation) or 100 penalty units or 5 years imprisonment, or both (in any other case).

This prohibition does not apply to the installation, use or maintenance of a tracking device in accordance with a warrant, emergency authorisation, corresponding warrant or corresponding emergency authorisation,

Section 10 of the SD Act provides:

> (1) A person must not knowingly install, use or maintain a data surveillance device on or in premises to record or monitor the input of information into, or the output of information from, a computer on the premises if the installation, use or maintenance of the device involves:
>
> (a) entry onto or into the premises without the express or implied consent of the owner or occupier of the premises, or
>
> (b) interference with the computer or a computer network on the premises without the express or implied consent of the person having lawful possession or lawful control of the computer or computer network.
>
> Maximum penalty: 500 penalty units (in the case of a corporation) or 100 penalty units or 5 years imprisonment, or both (in any other case).

This prohibition does not apply to the installation, use or maintenance of a data surveillance device in accordance with a warrant, emergency

authorisation, corresponding warrant or corresponding emergency authorisation.

Section 11 prohibits a person from publishing or communicating to any person, a private conversation or a record of the carrying on of an activity, or a report of a private conversation or carrying on of an activity, that has come to the person's knowledge as a direct or indirect result of the use of a listening device, an optical surveillance device or a tracking device in contravention of a provision of this Part and section 12 prohibits the possession of a record of private conversation or activity.

Section 14 prohibits a person from publishing or communicating to any person, any information regarding the input of information into, or the output of information from, a computer obtained as a direct or indirect result of the use of a data surveillance device in contravention of this Part.

The method and grounds of an application for such a warrant are set out in section 17 of the SD Act:

> (1) A law enforcement officer (or another person on his or her behalf) may apply for the issue of a surveillance device warrant if the law enforcement officer on reasonable grounds suspects or believes that:
>
> (a) a relevant offence has been, is being, is about to be or is likely to be committed, and
>
> (b) an investigation into that offence is being, will be or is likely to be conducted in this jurisdiction or in this jurisdiction and in one or more participating jurisdictions, and
>
> (c) the use of a surveillance device is necessary for the purpose of an investigation into that offence to enable evidence to be obtained of the commission of that offence or the identity or location of the offender.
>
> (2) The application may be made to:
>
> (a) an eligible Judge in any case, or

(b) an eligible Magistrate in the case of an application for a surveillance device warrant authorising the use of a tracking device only.

(3) An application:

(a) must specify:

(i) the name of the applicant, and

(ii) the nature and duration of the warrant sought, including the kind of surveillance device sought to be authorised, and

(b) subject to this section, must be supported by an affidavit setting out the grounds on which the warrant is sought.

(4) If a law enforcement officer believes that:

(a) the immediate use of a surveillance device is necessary for a purpose referred to in subsection (1) (c), and

(b) it is impracticable for an affidavit to be sworn before an application for a warrant is made, an application for a warrant may be made before an affidavit is prepared or sworn.

(5) If subsection (4) applies, the applicant must:

(a) provide as much information as the eligible Judge or eligible Magistrate considers is reasonably practicable in the circumstances, and

(b) not later than 72 hours following the making of the application, send a duly sworn affidavit to the eligible Judge or eligible Magistrate, whether or not a warrant has been issued.

(6) An application for a warrant is not to be heard in open court.

Section 19 sets out the matters upon which the eligible judge must be satisfied:

(1) An eligible Judge or eligible Magistrate may issue a surveillance device warrant if satisfied:

(a) that there are reasonable grounds for the suspicion or belief founding the application for the warrant, and

(2) In determining whether a surveillance device warrant should be issued, the eligible Judge or eligible Magistrate must have regard to:

(a) the nature and gravity of the alleged offence in respect of which the warrant is sought, and

(b) the extent to which the privacy of any person is likely to be affected, and

(c) the existence of any alternative means of obtaining the evidence or information sought to be obtained and the extent to which those means may assist or prejudice the investigation, and

(d) the extent to which the information sought to be obtained would assist the investigation, and

(e) the evidentiary value of any information sought to be obtained, and

(f) any previous warrant sought or issued under this Part or a corresponding law (if known) in connection with the same offence.

The term "law enforcement agency" includes the Independent Commission Against Corruption, and "law enforcement officer" means, in relation to the Independent Commission Against Corruption—an officer of the Commission within the meaning of the *Independent Commission Against Corruption Act 1988*.

The contents of such a warrant are prescribed by section 20:

(1) A surveillance device warrant must:

(a) state that the eligible Judge or eligible Magistrate is satisfied of the matters referred to in section 19(1) and has had regard to the matters referred to in section 19(2), and

(b) specify:

(i) the name of the applicant, and

(ii) the alleged offence in respect of which the warrant is issued, and

(iii) the date the warrant is issued, and

(iv) the kind of surveillance device authorised to be used, and

(v) if the warrant authorises the use of a surveillance device on or in premises or a vehicle—the premises or vehicle on or in which the use of the surveillance device is authorised, and

(vi) if the warrant authorises the use of a surveillance device in or on an object or class of object—the object or class of object in or on which the use of the surveillance device is authorised, and

(vii) if the warrant authorises the use of a surveillance device on or about the body of a person—the name of the person, and

(viii) if the warrant authorises the use of a surveillance device in respect of the conversations, activities or geographical location of a person—the name of the person (if known), and

ix) the period during which the warrant is in force, being a period not exceeding 90 days, and

(x) the name of the law enforcement officer primarily responsible for executing the warrant, and

(xi) any conditions subject to which premises or vehicle may be entered, or a surveillance device used, under the warrant.

(2) In the case of a warrant referred to in subsection (1)(b)(vii), if the identity of the person is unknown, the warrant must state that fact.

(3) A warrant must be signed by the eligible Judge or eligible Magistrate issuing it and include his or her name.

(4) If an eligible Judge or eligible Magistrate issues a warrant on a remote application:

(a) the eligible Judge or eligible Magistrate must inform the applicant of:

(i) the terms of the warrant, and

(ii) the date on which and the time at which the warrant was issued, and cause those details to be entered in a register kept by the Judge or Magistrate for that purpose, and

(b) the Judge or Magistrate must provide the applicant with a copy of the warrant as soon as possible.

5 ICAC'S SYSTEMS TO CONTROL AND REGULATE THE APPLICATION FOR AND USE OF SURVEILLANCE DEVICE WARRANTS

The Commission's Operations Manual contains two Procedures regarding surveillance device warrants. The first is Procedure 10A entitled "Procedures for Obtaining and Executing Surveillance Device Warrants", the second is Procedure 10B entitled "Procedures for Use and Recording Surveillance Devices Act Information". Both were approved on 10 April 2008 and the former was amended on 19 August 2008.

Procedure 10A contains general information regarding the definition of the surveillance devices, sets out the circumstances when a warrant is required and the process for obtaining such a warrant. It specifies that in all cases the following steps will be followed:

1. The Case Officer will discuss with the Case Lawyer (if there is no Case Lawyer the Executive Director, Legal will assign one) to determine whether or not a warrant is required for the proposed use of a surveillance device or device is.

2. The Case Officer will obtain the approval of the Executive Director, ID to make an application. The approval is to be recorded on the Authorisation Checklist which is at Appendix A of the Procedure.

3. If approval is given for an application the Case Officer (includes nominated Lead Investigator) will notify the Chief Investigator, Surveillance and Technical Unit (STU), by e-mail outlining the requested tasking, investigation objectives, timings, potential risks, numbers and types of surveillance devices likely to be required and whether any are to be installed on persons, premises, objects or vehicles. The e-mail is to be copied to the Case Lawyer.

4. Where it is proposed to install a surveillance device on the premises, an object or a vehicle the Executive Director, ID, will decide whether the STU should be responsible for the installation or whether an outside agency will be asked to assist.

5. Once the Executive Director, ID has given approval for the use of the surveillance device(s) the Case Officer will obtain the sequential warrant number from the Chief Investigator, STU.

5 [Sic]. The Case Officer will advise the Case Lawyer of approval and, using the approved pro forma, prepare the affidavit in support of the application, the application and the warrant.

6. The Case Officer will ensure that the affidavits:

- discloses all relevant material facts, and
- addresses the following matters under section 19(2) of the SD Act, being the matters which must be considered by the judge/magistrate:

  a. The nature and gravity of the alleged offence in respect of which the warrant is sought;

  b. The extent to which the privacy of any person is likely to be affected;

  c. The existence of any alternative means of obtaining the evidence or information sought to be obtained and the extent to which those means may assist or prejudice the investigation;

  d. The extent to which the information sought to be obtained would assist the investigation;

  e. The evidentiary value of any evidence sought to be obtained; and

  f. Any previous warrant sought or granted under the SD Act or corresponding law (if known) in connection with the same offence.

7. Once prepared the Case Officer will submit the draft documents to the Case Officer's Chief Investigator for checking for factual accuracy.

8. The Chief Investigator will submit the draft documents and the Authorisation Checklists to the Case Lawyer.

9. The Case Lawyer is responsible for preparing:

a. the notification to the Attorney General under section 51 of the SD Act.

b. the affidavit deposing to the service of the section 51 notification.

10. The Case Lawyer will ensure that:

- all documentation meets the requirements of the SD Act; and
- sufficient grounds are made out in the affidavit to support the application.

11. Once settled by the Case Lawyer the draft documentation is to be referred to the Executive Director, Legal, for approval. Approval is to be recorded on the Authorisation Checklist.

12. Once the application is approved by the Executive Director, Legal the Case Lawyer is responsible for arranging service of the section 51 notification.

13. Once approved, the Case Lawyer will arrange for the application to be signed and the affidavit sworn by the Case Officer who is the law enforcement officer for the purpose of the application.

14. Once the Solicitor General has responded to the section 51 notification the Case Lawyer will complete the affidavit of service annexing the notification and a copy of the Solicitor General's advice.

15. The Case Lawyer will then make an appointment with the Common Law Duty Judge or, if the warrant is only for a tracking device and it is more convenient to do so, an eligible magistrate.

16. The Case Lawyer and deponent to the affidavit should attend the judge/magistrate. The following documents are placed before the judge or magistrate during the hearing of the application:

a. The affidavit deposing to the service of the section 51 notification;

b. The application;

c. The affidavit in support of the application and, if the judge indicates that he is prepared to grant the warrant sought;

d. The draft warrant.

17. If the application is granted the originals of the affidavits and application and a copy of the warrant (not the original warrant, which must be returned to the Commission) are then placed in a sealed envelope by the judge's associate/magistrate and retained on the courts file.

18. Upon return to the Commission the Case Lawyer will give the original warrant together with copies of all supporting documentation and the authorisation checklists to the Chief Investigator SDU who will arrange for registration and retention of the documentation.

19. Upon notification that a warrant has been issued for the use of a surveillance device or devices an ICS case note should be prepared by the Case Officer indicating the time and date the warrant was issued, together with the expiry date and name of the issuing judge/magistrate. The Case Officer is to ensure that the Product Management Officer in STU is notified of the issue of the warrant. The Product Management

Officer will create a task on 'Outlook' for 'submit section 44 report' and initiate an automatic expiry date reminder alert so as to enable the Case Lawyer sufficient time to prepare the section 44 Report.

Procedure 10A then goes on to set out the steps to be followed for urgent situations, extension or variation of a warrant, revocation of warrant, retrieval of devices, and section 44 reports. In addition the procedures for execution of the warrant, equipment, logs, disk handling care and storage, protection of surveillance device technologies and methods, transcription and notifying the subject of the surveillance are set out.

The Procedure requires the Chief Investigator STU to:

a. ensure the highest degree of security is afforded to the storing of all surveillance devices,

b. be responsible for the installation, operational servicing and recovery of surveillance devices in accordance with warrants issued under the SD Act.

c. liaise with any relevant outside agency regarding the installation, servicing and recovery of any device installed by that agency,

d. purchase, modify, manufacture and provide surveillance device equipment and maintain a register of all such equipment in possession of the Commission. The register is to include sufficient details of all surveillance devices to ensure accurate identification,

e. ensure that relevant STU officers are trained in the use and installation of the surveillance devices and that sufficient STU members are available for immediate call,

f. audit the register of surveillance devices equipment quarterly. Details of any losses, thefts, damage, destruction and device is outstanding at the expiration of a relevant warrant, must be brought to the attention of the Executive Director, ID.

Procedure 10B addresses the strict limitations imposed by section 40 of the SD Act on the use of "protected information", the record keeping requirements imposed by subsections 44, 46 and 47 of the SD Act and also the requirement

to destroy any record or report obtained by use of a surveillance device under section 41(1)(b) of the SD Act.

6 TRUTH OF THE CONTENTS OF AFFIDAVITS

A further aspect requiring consideration is whether the contents of the affidavits in support of the applications for warrants are true to the best of the applicant's knowledge and belief.

It is neither possible nor practicable to cross-examine every deponent upon every affidavit. However, examination of the facts set out in the affidavits in support reveals that the belief was held by reason of information obtained from individuals, lawfully obtained telephone intercepts or surveillance devices or from the results of previous searches. The results of these prior activities are registered and recorded within the premises of the ICAC and any discrepancy between the contents of the affidavit and those records would be readily apparent to the senior officers whose approval is required. Furthermore, an examination of each application shows an internal consistency of information together with internal support for the conclusions derived and raises a high degree of probability that the contents of those affidavits were true and correct.

7 CASE STUDIES

Reports into two of the cases studied have been published. In respect of the remaining matters the description of the facts of each case has been considerably abbreviated to prevent publication of any prohibited information.

In each of the cases studied there has been complete compliance with the formal requirements of sections 17, 20, 44 and 51 of the SD Act.

In addition, the requirements of ICAC's own Procedures 10A and 10B appear to have been fully followed including the Authorisation Checklist.

Warrant No. SDW1 of 2009. Operation Garland (E08/0844)

This warrant was issued on 2 February 2009 and authorised the use of two listening devices as well as a tracking device to be located on a motor vehicle.

The affidavit in support of the application for the warrant revealed that as a result of information received it was reasonably suspected that a person acting on behalf of a Government Agency was unlawfully soliciting bribes in return for a benefit which he was in a position to give.

To obtain evidence to support the suspicion it was arranged that a controlled operation would take place in which an officer of the ICAC would pose as a person seeking the benefits which the target was able to provide. It was anticipated that the target would solicit a bribe from that officer.

To secure such evidence the Commissioner authorised pursuant to section 8 of the *Law Enforcement (Controlled Operations) Act* 1997 (NSW) a named person as a law enforcement participant for the purpose of investigating the relevant offence.

That person was to have listening devices on him. In addition the tracking device was to identify the location of the vehicle in which the controlled operation was being conducted throughout its course. This was to enable the Commission to maintain constant physical and some video surveillance of the vehicle which would be in motion during the operation.

The relevant offence in respect of which the warrant was issued was that the target person corruptly solicited a benefit contrary to section 249B(1) of the Crimes Act in return for falsely certifying certain matters.

The warrant was revoked on 20 February 2009. The affidavit in support of the application for revocation of the warrant states that the warrant was obtained for use during the controlled operation which was completed on 10 February 2009 and no further controlled operations would be conducted in relation to the investigation. In particular it states that the investigation was, by the date of the affidavit (20 February 2009) in an overt phase and the tracking device was no longer required.

A report on file into the use of the surveillance device shows that be tracking device was installed in a vehicle at 10:00 on 10 February 2009, activated at that time and de-activated at 18.02 on the same day.

Warrant No. SDW2 of 2009. (File E08/2483)

This warrant was issued on 24 February 2009 and authorised the use of an optical surveillance device upon certain premises.

As a result of information received it was believed on reasonable grounds that

one or more persons were corruptly receiving money from fellow employees of a Government Agency in return for being allowed to do less work for their common employer than would otherwise be required. It was believed on reasonable grounds on the basis of the information received that such payments were made by leaving them in a bag in a specific room to which access could be gained only by those involved in the allegedly corrupt activity. This would amount to the offence of corruptly receiving a benefit contrary to section 249B(1) of the Crimes Act.

To obtain evidence of such payments the warrant was sought so that optical surveillance could be maintained over the room in question.

The report under section 44(1) of the SD Act reveals that the optical surveillance device was used between 11:39 am on 10 March 2009 and 8:00 am on 7 April 2009 and that no direct evidence was obtained of the alleged offence and no use was to be made of the information obtained.

The notice under section 51(1) of the SD Act was served on the solicitor general on 24 February 2009 and was acknowledges on the same day. The warrant was revoked on 17 April 2009.

Warrant No. SDW3 of 2009. Operation Bauer (E09/0394)

As the results of this investigation have been made public by report published in June 2009 it is proposed to go into some detail.

On 10 March 2009 two officers of Warringah Council attended premises at Dee Why to inspect them prior to approval of a development application for

their use as a supermarket/butcher. The applicants Jin Hua Chen and Yu Ling Sun were in attendance at the time.

Towards the end of the inspection of the premises and away from one of the Council officers Ms Sun placed an envelope into the back pocket of one of the Council officers. He immediately retrieved it, opened it and saw that it contained at least three $50 banknotes. He returned the envelope to Ms Sun. Upon their return to the Council the officers reported the incident. The Council then informed the ICAC.

As a result of this information it was proposed to conduct a controlled operation under the *Law Enforcement (Controlled Operations) Act* 1997 involving an officer of the Council as a civil participant for the purpose of investigating the relevant offence namely that Yu Ling Sun corruptly offered a benefit contrary to section 249B(2) of the Crimes Act in return for obtaining approval of a building inspection required to operate the relevant premises as a supermarket/butcher.

It was proposed to arrange a meeting between the officer and Ms Sun which may also be attended by Mr Chen. At the meeting the Council officer would enquire as to the nature and purpose of the money given to the officer and if the other envelope that Sun had in her possession on that day was intended for him, what it contained and what her intentions were. It was intended that the meeting would be between the Council officer, Sun and Chen in the office of the Warringah Council Internal Ombudsman at the Warringah Council premises.

It was proposed to use listening devices plus an optical surveillance device for the purpose of recording the conversations and interactions between the

Council officer, Ms Sun, Mr Chen and any of their associates which may take place during the course of the controlled operation.

The warrant was issued on 19 March 2009 authorising the use of listening devices and one optical surveillance device.

The report in accordance with section 44(1) of the SD Act states that one of the listening devices was used to record meetings which took place on 20 and 23 March 2009. The optical surveillance device was not used.

The evidence obtained by use of the surveillance devices was used to progress the Commission's investigation and will be provided to the Director of Public Prosecutions in future prosecution proceedings against Sun and Chen.

A reading of the published report shows that a Council officer operating under the controlled operation obtained evidence of conversations at the premises at Dee Why by means of the listening devices. The optical surveillance device was not used.

Nonetheless the information obtained by use of listening devices contributed towards the findings of the Commission that on 10 March 2009 Sun with the agreement of Chen handed an envelope containing $200 to a Council officer with the intention of facilitating the building inspection approval for the Dee Why premises. Furthermore the Commission found that on each of 20 and 23 March 2009 Mr. Chen handed an envelope containing $200 to a Council officer with the intention of expediting the building inspection approval process for the Dee Why premises. Ms Sun was aware of and complicit in the provision of the money on 20 March 2009.

Recommendations were made that the advice of the Director of Public Prosecutions should be obtained with respect to the prosecution of Chen for three offences of corruptly offering an inducement under section 249B(2) of the Crimes Act and of Ms Sun for two offences of corruptly offering an inducement under section 249B(2) of the Crimes Act.

Warrant No. SDW6 of 2009. Operation Chaucer (E09/0591)

This operation is now the subject of a report of investigation into the solicitation and receipt of corrupt payments from a RailCorp contractor published in September 2009.

As a result of the information received from Mr Anes Harambasic, the proprietor and manager of Unisec Security Pty. Ltd (Unisec), and from lawfully intercepted telephone conversations it was believed on reasonable grounds that a person calling himself Yusuf (later established as being Mohammed Ali) was attempting to solicit money from him in return for securing a contract for provision of security guard auditing services with RailCorp. This is the offence of corruptly soliciting a benefit contrary to section 249B(1) of the Crimes Act. Further investigation revealed that Mohammed Ali was acting on behalf of Wasim Khan who was then employed by RailCorp as a Procurement Manager.

To identify those who were engaged in this activity and to establish the full extent of their involvement, it was necessary to make extensive use of covert physical and electronic surveillance. This included a number of telecommunications interceptions pursuant to warrants under the *Telecommunications (Interception and Access) Act 1979* (Cwlth) and the use of surveillance devices authorised by warrants obtained under the SD Act. A controlled operation was also authorised under the *Law Enforcement*

(Controlled Operations) Act 1997 (NSW). A controlled operation permits those authorised under the operation to engage in specified activity which would otherwise be unlawful. By this stage Yusuf, whom the Commission had now identified as Mohammed Ali, had asked for money in return for assistance being provided to Unisec to win the RailCorp contract.

The controlled operation was conducted with the assistance of Mr Harambasic. It involved Mr Harambasic attending a meeting requested by Wasim Khan's cousin, Tabrez Khan, who was also operating under an alias, and making a payment of $15,000 to Tabrez Khan. In addition, the Commission lawfully executed three search warrants as a result of which further documents and the $15,000 cash paid to Tabrez Khan were seized. The Commission also conducted three compulsory examinations of witnesses in order to further clarify matters.

At the time of applying for this warrant under the SD Act on 27 April 2009, the involvement of Wasim Khan had not been established. The primary person of interest was then Mohammed Ali.

For the purpose of investigating this offence and to enable the collection of evidence of the commission of the offence it was considered necessary to apply for a warrant for the use of a tracking device to be located on the motor vehicle which was then used by Mohammed Ali to enable the ICAC's officers to identify his whereabouts.

The Commission had previously used physical surveillance of him. However on 17 April 2009 a Commission officer was assaulted by a person living in the neighbourhood of Ali. Also he had displayed a tendency to swap telephone services when contacting Mr Harambasic indicating that he was surveillance

aware which would render physical surveillance alone without the added benefit of using a tracking device less effective as an investigation technique.

The warrant was issued on 27 April 2009.

Application was made on 2 July 2009 for the revocation of the warrant on the ground that the use of the device authorised was no longer necessary for the purpose of enabling evidence to be obtained of the commission of the relevant offence or the identity or location of the person of interest.

The report under section 44(1) of the SD Act shows that it was installed on the subject vehicle on 5 May 2009 at 7:30 pm and retrieved on 22 May 2009 and 6:45 pm. The movement of the vehicle was recorded between those times.

The use of the warrant contributed to the Commission's findings that Wasim Khan arranged for the Unisec tender to be increased from about $115,000 per annum over four years to about $180,000 per annum, so that Unisec would be able to afford to make $200,000 in corrupt payments over four years to Wasim Khan. Corrupt conduct findings are made against Wasim Khan, Mohammed Ali and Tabrez Khan.

The Commission was of the opinion that consideration should be given to obtaining the advice of the Director of Public Prosecutions with respect to:

- the prosecution of Wasim Khan for offences of soliciting a corrupt benefit of $200,000 and receiving a corrupt benefit of $15,000 contrary to section 249B(1) of *the Crimes Act 1900 (NSW)* (the Crimes Act)
- the prosecution of Mohammed Ali for an offence of aiding and abetting the soliciting of a corrupt benefit contrary to section 249F of the Crimes Act, and

- the prosecution of Tabrez Khan for an offence of aiding and abetting the soliciting of a corrupt benefit and an offence of aiding and abetting the receiving of a corrupt benefit, contrary to section 249F of the Crimes Act.

The investigation also identified inadequately trained staff as the major risk area that made it possible for the corrupt conduct to occur and the Commission made five recommendations to improve RailCorp procurement systems and procedures in order to prevent future opportunities for corruption.

Warrant No. SDW7 of 2009.

On 4 May 2009 (the date of the issue of this warrant) it was believed that the target was likely to be providing relevant and confidential information to another person in a corrupt scheme to solicit money..

The warrant authorised the use of a tracking device on a motor vehicle used by the target to enable the Commission's investigators to identify meetings relating to the offence.

The report in accordance with section 44(1) of the SD Act says that no movement was recorded by use of the tracking device.

Warrant No. SDW8 of 2009. Operation Siren (E09/1228)

A citizen complained to the ICAC that bribes were being demanded of him by an officer of a Government Agency in return for benefits to be provided to that citizen.

To obtain evidence of this corrupt conduct which constitutes an offence under section 249B(1) of the Crimes Act application was made for the issue of a warrant under the SD Act for the use of the following surveillance devices:

- On or in certain premises: three listening devices and one optical surveillance device
- On or in further premises: one optical surveillance device
- On or in a motor vehicle driven by the person alleged to be soliciting bribes: one tracking device
- On or in a motor vehicle driven by the citizen: three optical surveillance devices
- On or about the body of the citizen: three listening devices and one optical surveillance device.

It was anticipated that a meeting would take place between the citizen and the person alleged to be seeking bribes during a controlled operation. The premises nominated were identified as the best location for using optical surveillance devices. The information sought to be obtained by reason of these devices would assist the investigation of the relevant offence by providing evidence of corrupt payments involving the alleged bribe demander and also provide evidence or intelligence of his movements including his involvement in corrupt activities with other as yet unknown participants.

The warrant was issued on 30 July 2009.

The report in accordance with section 44(1) of the SD Act shows that the devices were in fact used and that useful information was obtained from all surveillance devices and this information is informing the ongoing investigation.

8 CONCLUSION

In the six cases studied no application was made for the issue of a data surveillance device. In four of the cases warrants issued for tracking surveillance devices which were used except for one. In three cases warrants issued for the use of optical surveillance devices which were used except for one.

In many cases the Commission's mode of investigating a complaint of criminal corruption involved a controlled operation authorised under the *Law Enforcement (Controlled Operations) Act 1997(NSW)*. A controlled operation permits those authorised under the operation to engage in specified activity which would otherwise be unlawful. In the controlled operation a civil participant would covertly record conversations with the suspect by means of the use of a listening device authorised by a warrant issued under the SD Act. To provide some corroboration of the meeting between the civil participant and the suspect it would be recorded by means of the use of an optical surveillance device authorised by a warrant issued under the SD Act. In appropriate cases it was necessary to track the movements of a suspect by

means of the use of a tracking device authorised by a warrant issued under the SD Act.

A decision as to which of the devices will be used is, of necessity, made before the actual circumstances of their use is known to the Commission's officers. Consequently it is understandable that, at times, the actual circumstances may render the use of one or more of the devices unnecessary. This does not mean that the decision to apply for a warrant was unreasonable or improper.

The Commission has instituted and maintained a detailed and impressive system of controls designed to prevent the unauthorised or "rogue" application for a warrant under the SD Act in its Procedures 10A and 10B.

It achieves this goal by requiring the participation of a number of its officers from different sections in the approval process. Those officers include the Case Officer, the Case Lawyer, the Executive Director ID, the Chief Investigator of the Surveillance and Technical Unit (STU), the Case Officer's Chief Investigator, the Executive Director Legal and the Product Management Officer in the STU. The approvals of the Executive Directors of Investigations and Legal are required to be noted and actually appear on the Authorisation Checklist which accompanies the documentation.

In addition, the SD Act requires notification upon the Attorney General seeking approval for the application for a warrant and the reply from the Solicitor General.

The Procedures set out clear duties upon officers regarding the registration and retention of the documentation after the warrant has been authorised by the judge.

I have, pursuant to section 57B(2) of the ICAC Act, looked to see if there are grounds for reporting the existence of evidence of abuse of power, impropriety, or other forms of misconduct on the part of the Commission or officers of the Commission under section 57B(1)(b). I have also looked to see if there were grounds for reporting the existence of evidence of maladministration including unreasonable invasions of privacy and action or inaction of a serious nature that is contrary to law, unreasonable, unjust, oppressive or improperly discriminatory or based wholly or partly on improper motives under section 57B(1)(c).

In addition I have attempted to assess the effectiveness and appropriateness of the procedures of the Commission relating to the legality or propriety of its activities under section 57B(1)(d).

Examination of the application for and execution of surveillance search warrants in each of the cases studied reveals the following:

- Surveillance Device warrants (limited to tracking and optical devices) were applied for and used as one of the tools authorised by the ICAC Act to enable the ICAC to carry out its functions;

- Each warrant was applied for only in circumstances where a belief was reasonably formed in the light of information available from other sources that the application was soundly based;

- In all cases it was appropriate to apply for and execute the surveillance device warrant in the light of the information then available;

- In all but those cases where execution was not undertaken or where execution revealed no evidential material, the issue and execution of the surveillance device warrants were effective in locating material which contributed to the investigations of the Commission;

- There was no evidence of abuse of power, impropriety, or other forms of misconduct on the part of the Commission or officers of the Commission;

- There was no evidence of maladministration, including unreasonable invasions of privacy, or of any action or inaction of a serious nature that was contrary to law, unreasonable, unjust, oppressive or improperly discriminatory or based wholly or partly on improper motives.

Harvey Cooper AM
Inspector