JOINT STANDING COMMITTEE ON THE CORRUPTION AND CRIME COMMISSION

REPORT OF THE PARLIAMENTARY INSPECTOR CONCERNING PROCEDURES ADOPTED BY THE CORRUPTION AND CRIME COMMISSION RELATING TO SURVEILLANCE DEVICES

Report No. 12
in the 38th Parliament

2010

Published by the Legislative Assembly, Parliament of Western Australia, Perth, November 2010.

Joint Standing Committee on the Corruption and Crime Commission

Report of the Parliamentary Inspector concerning Procedures Adopted by the Corruption and Crime Commission relating to Surveillance Devices

ISBN: 978-1-921865-05-3

(Series: Western Australia. Parliament. Legislative Assembly. Committees.
Joint Standing Committee on the Corruption and Crime Commission. Report 12)

328.365

99-0

JOINT STANDING COMMITTEE ON THE CORRUPTION AND CRIME COMMISSION

REPORT OF THE PARLIAMENTARY INSPECTOR CONCERNING PROCEDURES ADOPTED BY THE CORRUPTION AND CRIME COMMISSION RELATING TO SURVEILLANCE DEVICES

Report No. 12

Presented by:
Hon Nick Goiran, MLC and John Hyde, MLA
Laid on the Table of the Legislative Council and Legislative Assembly
on 18 November 2010

COMMITTEE MEMBERS

Chairman	Hon Nick Goiran, BCom, LLB, MLC Member for the South Metropolitan Region
Deputy Chairman	John Hyde, BA, DipEd, JP, MLA Member for Perth
Members	Frank Alban, MLA Member for Swan Hills
	Hon Matt Benson-Lidholm, BA, DipEd, JP, MLC Member for Agricultural Region

COMMITTEE STAFF

Principal Research Officer	Scott Nalder, BJuris (Hons), LLB, BCL (Oxon)
Research Officer	Michael Burton, BEc, BA (Hons)

COMMITTEE ADDRESS

Joint Standing Committee on the Corruption and Crime Commission
Legislative Assembly
Parliament House
Harvest Terrace
PERTH WA 6000

Tel: (08) 9222 7494
Fax: (08) 9222 7804
Email: jscccc@parliament.wa.gov.au
Website: www.parliament.wa.gov.au/jscccc

TABLE OF CONTENTS

COMMITTEE'S FUNCTIONS AND POWERS

On 25 November 2008 the Legislative Council concurred with a resolution of the Legislative Assembly to establish the Joint Standing Committee on the Corruption and Crime Commission.

The Joint Standing Committee's functions and powers are defined in the Legislative Assembly's Standing Orders 289-293 and other Assembly Standing Orders relating to standing and select committees, as far as they can be applied. Certain standing orders of the Legislative Council also apply.

It is the function of the Joint Standing Committee to -

(a) monitor and report to Parliament on the exercise of the functions of the Corruption and Crime Commission and the Parliamentary Inspector of the Corruption and Crime Commission;

(b) inquire into, and report to Parliament on the means by which corruption prevention practices may be enhanced within the public sector; and

(c) carry out any other functions conferred on the Committee under the *Corruption and Crime Commission Act 2003*.

The Committee consists of four members, two from the Legislative Assembly and two from the Legislative Council.

CHAIRMAN'S FOREWORD

The Parliamentary Inspector has tabled a report with the Committee recommending that the *Surveillance Devices Act 1998* be amended to afford persons a statutory right to apply to the Supreme Court to obtain confirmation that a surveillance device, installed in their homes by the Corruption and Crime Commission (CCC), has been removed but that such a statutory right be confined to circumstances where it has been "acknowledged" that:

- a surveillance device has been installed by the CCC; and
- the CCC's investigation has come to an end.

It is clear that such an amendment would not be without consequence. At the heart of the issue is a need to balance the privacy concerns of the citizens of Western Australia with the fact that any move to require greater disclosure by the CCC might compromise future investigations undertaken by the CCC.

Ultimately, the Committee has decided not to express a view on the merits of the Parliamentary Inspector's proposed amendment, or the CCC's response. Instead the Committee has resolved to table, as appendices to this report, the following documents:

- the Parliamentary Inspector's report;
- the CCC's response; and
- the transcript of the closed hearing of the Committee with the Parliamentary Inspector in which his report was considered and his proposed amendment debated.

By this process the Committee seeks to put all relevant information before Parliament to enable an informed discussion on the Parliamentary Inspector's report and proposed amendment.

HON NICK GOIRAN, MLC
CHAIRMAN

CHAPTER 1 PARLIAMENTARY INSPECTOR'S REPORT

1.1 Tabling of Parliamentary Inspector's report with the Committee

The Corruption and Crime Commission (CCC) can apply to a judge for a warrant to record, monitor and listen to private conversations by way of the use of a surveillance device.[1]

On 15 September 2010 the Parliamentary Inspector of the Corruption and Crime Commission, the Honourable Chris Steytler QC, tabled a report with the Committee entitled *Report Concerning Procedures Adopted by the Corruption and Crime Commission relating to Surveillance Devices*.[2]

This report was prompted by an inquiry by the Parliamentary Inspector into the procedures adopted by the CCC in making use of surveillance devices. The Parliamentary Inspector initiated this inquiry after a person who was previously under investigation by the CCC complained on commercial television that the CCC would not disclose whether or not surveillance devices remained in place in or around that person's home.

The CCC's investigation concerning that person had ceased. The person then sought confirmation from the CCC that the surveillance device had been removed. The CCC, citing "operational reasons", refused to confirm whether or not the surveillance device had been removed.

The Parliamentary Inspector learned that the CCC has a policy of neither confirming, nor denying the use of surveillance devices and applied this policy in the case of the complainant.

The Parliamentary Inspector believes that the CCC's policy of non-disclosure should not have been inflexibly applied. He was not persuaded by the reasons given by the CCC in support of its refusal to depart, under any circumstances, from its policy.

In support of his position, the Parliamentary Inspector makes the observation that "[t]here can be few investigative techniques more intrusive than the use of surveillance devices in a private home".

---

1 *Surveillance Devices Act 1998*, s 15(1).

2 The Parliamentary Inspector can table such a report with the Committee or directly with Parliament. The current Parliamentary Inspector has indicated that his practice will be to table such reports with the Committee, in response to the Committee's preference that he does so. See the Committee's Report No 2 of the 38th Parliament, *Report on the Relationship between the Parliamentary Inspector and the Commissioner of the Corruption and Crime Commission*, which was tabled in Parliament on 19 March 2009 for the rationale underlying the Committee's preference.

The Parliamentary Inspector does not have the power to direct the CCC to change its policy, or apply its policy in a particular way. The Parliamentary Inspector can, however, make recommendations. In his report the Parliamentary Inspector has recommended that the *Surveillance Devices Act 1998* be amended to afford persons a statutory right to apply to the Supreme Court to obtain confirmation that a surveillance device, installed in their homes by the Corruption and Crime Commission (CCC), has been removed but that such a statutory right should be confined to circumstances where:

- it has been unequivocally acknowledged that a surveillance device has been installed by the CCC; and
- it has been acknowledged that the CCC's investigation has been finalised.

On 11 October 2010 the Committee met with the Parliamentary Inspector to discuss his report. Debate centred on the practicalities of the Parliamentary Inspector's proposed amendment. The Parliamentary Inspector conceded that his proposed amendment may raise potential problems in a limited range of circumstances, but the Parliamentary Inspector was firmly of the view that this did not detract from the importance of the matters his amendment sought to address.

Though it may be well understood by a number of the citizens of Western Australia, it bears mentioning that before obtaining a warrant to use a surveillance device in an investigation, the CCC must satisfy a judge both that an offence has been or may have been, is being or is about to be, or is likely to be, committed, and that the use of a listening device, an optical surveillance device, or a tracking device would be likely to assist an investigation into that offence or suspected offence, or to enable evidence to be obtained of the commission of that offence, or the identity or location of the offender.[3] Plainly, these are not simple requirements. Furthermore, any such warrant will by law be finite in duration and specific in purpose. During the 2009-10 reporting period, the CCC successfully applied for eight warrants to use surveillance devices for the purposes of its various investigations.[4]

Ultimately the Committee has decided not to express a view on the merits of the Parliamentary Inspector's proposal, or the CCC's response. Instead the Committee has resolved to table, as annexures to this report, the following documents:

- the Parliamentary Inspector's report;
- the CCC's response; and
- the transcript of the closed hearing of the Committee with the Parliamentary Inspector in which his report was considered and his proposed amendment debated.

---

3 *Surveillance Devices Act 1998*, s 13(1).

4 Corruption and Crime Commission of Western Australia, *Annual Report 2009 - 2010*, p 39.

1.2 Redactions to the Appendices

After consultation with the Parliamentary Inspector and the CCC, schedules 1-7 of the Parliamentary Inspector's original report have been removed due to operational sensitivity. The redacted version of the Parliamentary Inspector's report appears as Appendix One. Schedule 8 of the Parliamentary Inspector's report, being the CCC's response, has been reproduced as Appendix Two with certain amendments and redactions having been made to exclude operationally sensitive material. The transcript of the closed hearing of the Committee, which appears as Appendix Three, has also been redacted to exclude operationally sensitive material.

HON NICK GOIRAN, MLC
CHAIRMAN

APPENDIX ONE

REPORT CONCERNING PROCEDURES ADOPTED BY THE CORRUPTION AND CRIME COMMISSION RELATING TO SURVEILLANCE DEVICES

S 201 of the *Corruption and Crime Commission Act 2003 (WA)*

15 September 2010

This report concerns an assessment of the effectiveness and appropriateness of procedures adopted by the Corruption and Crime Commission ('CCC'). The assessment is made by me under s 195(1)(c) of the *Corruption and Crime Commission Act 2003 (WA)* ('CCC Act'). It is made on my own initiative, pursuant to s 195(2)(a) of the CCC Act.

The procedures in question

The procedures in question concern a policy adopted by the CCC in respect of surveillance devices under the terms of the *Surveillance Devices Act 1998 (WA)* ('SD Act'). Pursuant to this policy, the CCC declines to disclose to occupants of homes, in which surveillance devices have been installed by it pursuant to a since expired warrant, whether or not the surveillance devices remain in place. This policy is inflexibly applied in all cases, regardless of the circumstances, including circumstances in which the fact of installation of the devices has become publicly known and the investigation for the purposes of which they were installed is acknowledged to have been finalised.

Circumstances giving rise to the assessment

For the purpose of an investigation ('Investigation') conducted by it in 2006, the CCC applied for a warrant under the SD Act for the secret placement of optical surveillance and listening devices in the home of the persons identified in Schedule 1 to this report. The warrant was issued by the Supreme Court of Western Australia under s 13(3) of the SD Act. The Court must consequently have been satisfied that there were reasonable grounds for believing that:

1. 'an offence has been or may have been, is being or is about to be, or is likely to be, committed'; (s 13(1)(a)) and
2. 'the use of a listening device [or] ... an optical surveillance device ... would be likely to assist an investigation into that offence or suspected offence, or to enable evidence to be obtained of the commission of that offence, or the identity or location of the offender' (s 13(1)(b)).

The warrant (a copy of which is contained in Schedule 2 to this report) was in force for periods ending on 17 February 2007. It required that '[w]here practicable the surveillance device should be retrieved or rendered inoperable during the period that the warrant is in force'. For reasons that are not presently relevant, other than to say such disclosure was required by law, the existence and contents of the warrant were disclosed to the first of the persons mentioned in Schedule 1 ('A') on 26 September 2009. By that date the Investigation had long since been completed.

Prior to that date, it had become known to A and to the second of the persons mentioned in Schedule 1 ('B') that listening devices had been installed in their home. On 15 March 2007, B made a written request to the then Commissioner of the CCC, Commissioner Hammond, that the CCC's listening devices be removed from the family home. A copy of her letter comprises Schedule 3 to this report.

Mr Robert Sutton, the then Deputy Director of Operations of the CCC, responded to B' s letter on 27 March 2007, as follows:

> Surveillance devices installed by the Commission are installed pursuant to a warrant issued by a Judge of the Supreme Court of Western Australia under the *Surveillance Devices Act 1998 (WA).* This Act contains provisions that relate to the confidentiality of these applications. Additionally, for operational reasons, the Commission is unable to comment on the installation or removal of devices installed under warrant.
>
> Please note however, that the *Surveillance Devices Act* only enables agencies to install and monitor devices for a specified period, after which time a further application to the Supreme Court for an extension of the warrant is required. This would only be granted if the grounds to grant the warrant are still in existence.
>
> Unfortunately, the Commission is not in a position to provide you with any specific information about this subject.

Mr Sutton's response (which comprises Schedule 4 to this report) identified the policy which has since been adhered to by the CCC in subsequent correspondence with A and B's legal representative and with my predecessor in office, Mr McCusker AO QC, and Acting Commissioner Martin QC. Mr McCusker elected not to pursue the issue.

The exchange of correspondence referred to in the preceding paragraph reveals that the principal reasons offered in support of the CCC's policy were essentially as follows:

1. most law enforcement agencies in Australia use surveillances devices and the methodology used is closely guarded;
2. information about the technology and installation of surveillance devices has never been released by any law enforcement agency;
3. all law enforcement agencies in Australia employ the policy of neither confirming, nor denying, the use of surveillance devices;
4. should the CCC answer the question asked by A and B, the policy identified in point 3 would be compromised, potentially affecting the CCC's relations with other agencies;
5. witnesses before the CCC who have previously lied to it subsequently tell the truth when they realise that their conversations have been recorded by surveillance devices;
6. witnesses are more inclined to initially tell the truth if they believe their private conversations may have been subject to surveillance devices, whether this actually happened, or not;
7. if the CCC told an affected person that surveillance devices had been removed, but refused to answer a similar question later asked in respect of another case, that person would infer that he or she was under surveillance;

8. if the Commissioner told A and B whether or not the surveillance devices have been removed, the CCC could be subjected to similar enquiries; and
9. the three reasons identified in Schedule 5 to this report (which relate specifically to A and B).

The issue came to my attention shortly after 10 May 2010, on which date A had said on commercial television that he continued to ask the CCC whether or not surveillance devices remained in place in and around his home. He said that the CCC would not answer that question. Having learned of this, I confirmed that the facts were as stated by A and re-opened the issue.

By letter dated 11 May 2010, I wrote to Acting Commissioner Archer SC (the Commissioner was then on leave). I suggested that the CCC's continuing position was, on the face of it, unjustified and unnecessarily oppressive for the reasons given in my letter. My letter, and Ms Archer's reply to it dated 13 May 2010, are contained in Schedule 6 to this report (these have been redacted to remove sensitive, but not presently relevant, material). In her letter, Ms Archer maintained the CCC's refusal to answer the question posed by A and B. She offered three reasons in support of the CCC's policy, as follows:

1. It 'is neither sound operational practice nor usual for law enforcement agencies to either confirm or deny whether there is surveillance equipment in place or not. Such concessions create precedents about other cases.'
2. The Commission 'would be in a difficult position if, having certified that there were no devices present, it wished to deploy devices as a part of a new investigation at some point in the future.'
3. The CCC might be viewed as being 'deceptive' if, in circumstances in which a question of that kind had been answered by saying that surveillance devices had been removed, any other law enforcement agency subsequently found

However, in her letter, Ms Archer offered to write to A and B, saying, amongst other things, that:

> 'The Commission's use of the relevant surveillance under [previously identified] warrants complied with the requirements of the relevant Supreme Court warrants and the *Surveillance Devices Act 1998*. Accordingly, that equipment has either been removed, or cannot be activated or monitored without a further warrant being obtained to authorise that.'

She asked whether I was content with this text.

I responded by letter dated 20 May 2010, addressed to Acting Commissioner Shanahan SC (the Commissioner was still on leave and Ms Archer's acting role had concluded). I said that I was not content with the proffered text, for the reasons given in that letter (also redacted), a copy of which is Schedule 7 to this report. It is unnecessary to re-state those reasons in the body of this report. They sufficiently appear from my assessment below.

There followed exchanges of correspondence which culminated in my letter to the Commissioner under s 200 of the CCC Act dated 30 August 2010, to which I attached a copy of my draft report. By letter dated 7 September 2010, the Commissioner provided his final submission to me under s 200 of the CCC Act. The Commissioner's submission is Schedule 8 to this report.

My assessment

The issue raises difficult questions. There is undoubtedly considerable weight in some, at least, of the Commission's submissions. However, I am not persuaded by its reasons given in support of its refusal to depart, under any circumstances, from its policy of non-disclosure. My assessment is that the weight of the Commission's reasons does not outweigh the interests of persons in the position of A and B.

I can understand why the CCC might adhere to its policy in a case in which the person subjected, or possibly subjected, to the surveillance devices ('suspect') does not know whether or not use has been made of those devices or does not know whether or not the investigation that led to their use remains ongoing.

However, it is harder to justify a refusal, under any circumstances, to say whether a device has been removed once it is known by the suspect that it had been placed in his or her home and it is known, beyond any doubt, that the investigation for the purposes of which the necessary warrant was obtained has been completed (which is, of course, the case with A and B). I can see no reason why any operation of the CCC, present or future, might be jeopardised by an assurance that is limited to the particular warrant obtained by the CCC for the purpose of a particular investigation that is known to have been finalised. I have not sought any greater assurance than that.

Nor am I persuaded that, in circumstances of this limited kind, the giving of the confirmation sought would create an unacceptable precedent.

None of the matters raised by the CCC in paragraphs (a) to (c) on page 2 of Schedule 8 (essentially operational material concerning the technology and methodology used and the location of devices) would be revealed in the course of giving the limited assurance sought. The same is true of the similar matters identified in the last two paragraphs on page 2 of Schedule 8 and in the whole of page 3 of that schedule.

The comments in paragraphs (d) and (e) on page 2 of schedule 8 (addressing allied issues) consequently seem to me to be irrelevant to the limited issue raised. The same is true of the material contained in the last paragraph on page 4 and in the first two full paragraphs on page 5.

In the third full paragraph on page 5 of Schedule 8, the CCC contends that the need for non-disclosure of sensitive information concerning technology, methodology and placement has been recognised by statute and by the courts. It says that this helps inform its position with respect to the non-disclosure of information relating to the retrieval of a device. With respect, that is a non-sequitur. Acknowledgement that a device has or has not been removed in circumstances such as the present reveals nothing concerning technology, methodology or placement. Of course, if the device was to be removed in the presence of a suspect or third party, this might reveal sensitive information. However, there is no reason why this should ever occur.

As will become apparent, I do not recommend that there be any absolute right to be informed in any case in which the placement of a device pursuant to a since expired warrant has become publicly known. Nor does my recommendation contemplate that removal of any devices might take place in the presence of any person other than Commission officers.

Rather, my recommendation is only that there be a right, in a case such as the present, to apply to a court for disclosure of the fact of removal, or non-removal, of the devices installed pursuant to *that particular warrant* and, if they have not been removed, for an order for their removal subject

to such conditions as might be appropriate (including conditions facilitating secrecy concerning the removal process). In the course of hearing such an application the installer of the devices would have the protection against disclosure of confidential information afforded by the principle of public interest immunity. If additional protection is thought to be necessary, provision could be made accordingly.

In these circumstances, it also follows that the CCC's concerns, expressed on pages 5 and 6 of Schedule 8 (concern that disclosure, in a case in which a device has been removed, would be tantamount to confirming that no investigation is currently in place or in prospect), is misplaced. All that the person would know in such a case would be that the device placed under the now expired warrant was no longer still in place. This would not tell the person anything about any other device installed, or that might be installed, pursuant to a different warrant. In any event, the Commissioner's submission rests upon what might, with respect, be thought to be a very doubtful assumption - that it is desirable to leave a person who is not under investigation in a state of uncertainty concerning that fact and concerning the possibility of being under surveillance in his or her home.

Moreover, given that the person concerned is likely to come to know of the existence of the warrant in question, and of the installation of the devices in question, only after the finalisation of the particular investigation, it is likely to be a relatively rare case (having regard for the nature of the CCC's misconduct jurisdiction) in which there is any realistic prospect of a further warrant being obtained.

Of course, if the court declined to grant an application for disclosure, this might indicate to the applicant that an investigation was in place or in prospect. However, there would presumably only be a refusal of the application in one of two circumstances. The first is a case in which the devices installed pursuant to the original warrant had been reactivated pursuant to a later warrant. The second is a case in which, for some reason, it was not practical or desirable for the devices to be removed.

I do not know whether the former circumstance is realistic. If it is, this might give rise to an accurate inference (by some-one who is presumably already suspicious), but it would also highlight the potential for abuse. Moreover, given that there might be a range of circumstances in which an application for disclosure might be refused under any applicable legislative provision (including circumstances in which it was impracticable to remove a device, or impractical without risking the revelation of sensitive information concerning technology, methodology or placement), and no obligation to give reasons, it is difficult to see why anyone inference should be stronger than other available inferences.

If the former circumstance is not realistic, no difficulty will arise.

In the latter circumstance, any inference drawn from the refusal of the application would probably be misplaced.

On the other hand, if there should be no right to bring an application of this kind, a person who is no longer under investigation, and not likely ever to be so again, would never have the comfort of knowing that his or her home was free of unlawful surveillance.

The concern that others might seek similar disclosures seems to me also to be misplaced. The statutory right would be given only in cases in which it was known (and acknowledged by the

CCC) that a device had been installed pursuant to a now expired warrant. That would encompass a very small class of people, each of whom should, in my opinion, be given the right to apply for disclosure.

The intractable approach taken by the CCC seems to me to undervalue important policy considerations.

There can be few investigative techniques more intrusive than the use of surveillance devices in a private home, more especially when both listening devices and optical surveillance devices are made use of. That is presumably why the SD Act effectively requires a court considering an application for a warrant for a listening device or an optical surveillance device to have regard to (s 13(2)):

(a) the nature of the offence or suspected offence in respect of which the warrant is sought;

(b) the extent to which the privacy of any person is likely to be affected by the use of a surveillance device under the warrant;

(c) the extent to which evidence or information is likely to be obtained by methods of investigation not involving the use of a surveillance device;

(d) the intelligence value and the evidentiary value of any information sought to be obtained;

(e) any other warrants sought or issued under this Act or the Listening Devices Act 1978 in connection with the same matter; and

(f) the public interest.

It is also presumably the reason why s 13(8)(f) and s 13(8)(h) of that Act requires the warrant to specify:

- the period that the warrant is in force, being in every case a period not longer than 90 days; (subs (f)) and
- that, where practical, the surveillance device should be retrieved or rendered inoperable during the period that the warrant is in force (subs (h)).

It is correct to say, as the CCC does, that the SD Act does not compel the CCC to disclose to a person affected whether or not surveillance devices remain in place. However, nor does it prevent the CCC from doing so if circumstances arise to justify this.

It is also true that the person affected can take some comfort from the requirements of ss 13(8)(f) and (h) of the Act. However, the thought that devices (which, in any case, might be optical as well as listening devices) might still be in place, even if not currently operating, would be unsettling. The devices constitute an intrusion into private property and knowledge that they might still be present would leave the householders with a sense of continuing unease or mistrust (whether misplaced or not) that they might be unlawfully re-activated. That unease or mistrust could have a significant effect upon the householders' ability to enjoy, and feel secure in, their own home. That has been so in the case of A and B, and continues to be so.

The CCC's policy must be considered against a background in which the individuals affected might already have suffered a very serious and possibly lengthy invasion of their privacy encompassing the secret observation of potentially embarrassing (but entirely legal) activities and

the secret overhearing of every private conversation. In the case of B, this invasion of privacy over a substantial period of time did not result in a conviction for the criminal offence alleged by the CCC in the originating warrant, or for any other offence. For persons to be left in a situation in which they will never know, at least with complete confidence, whether their family home is free of surveillance devices, whether presently operating or not, might, in some circumstances, be entirely unjustifiable.

It consequently seems to me that the inflexible operation of the CCC's policy is inappropriate, given that it is capable of an unnecessarily oppressive operation and takes what is already a fundamental (if sometimes necessary) inroad into the rights of the individual further than is justified.

My recommendation

I recommend that consideration be given to amending the provisions of the SD Act. An appropriate amendment might enable a person in a position similar to that in which A and B find themselves (where it has been unequivocally acknowledged that a surveillance device had been installed pursuant to a now expired warrant) to make an application to the Supreme Court for an order requiring the CCC to disclose whether the device remains in place and, if so, for an order that it be removed. The amendment might include provisions having the effect that:

1. an order for removal is not to be made unless subject to conditions that will ensure that secrecy is maintained concerning sensitive operational or technical information, including information relating to:

   (a) the technology used;

   (b) the methodology used; and

   (c) the location, in the premises, of any device;

2. an order for disclosure must not be made in circumstances in which the court is satisfied that it is not in the public interest for it to do so, or where it is satisfied that it is impractical for the device or devices to be retrieved; and

3. the court is not required to give reasons for its decision.

The principle of public interest immunity would apply to confidential information made use of in any such application. If further protection is thought to be necessary, it could be provided for.

The proposed amendment affords very limited, but nonetheless important, protection of basic civil rights.

Because I have not consulted any agency other than the CCC it might be appropriate for further consultation to be made before settling upon the terms of an amendment, if that course of action should be thought appropriate.

C D STEYTLER QC
PARLIAMENTARY INSPECTOR

APPENDIX TWO

REPRESENTATIONS OF THE CORRUPTION AND CRIME COMMISSION ON THE DRAFT REPORT CONCERNING PROCEDURES ADOPTED BY THE CORRUPTION AND CRIME COMMISSION RELATING TO SURVEILLANCE DEVICES

This is the Commission's submission in response to the draft report entitled *Report Concerning Procedures Adopted by the Corruption and Crime Commission Relating to Surveillance Devices.*

On its face, the proposition urged upon the Commission is a simple one, which arguably should sensibly lead to only one answer.

The proposition is that where surveillance devices have been lawfully used in a Commission investigation, then once that fact has been made publicly known and the particular investigation is acknowledged to have been finalised, there could be no prejudice to present or future operations of the Commission by it confirming to the persons the subject of that investigation that the devices have been removed.

However in the Commission's view, it is critical that the proposition be examined in its true operational context - and when that is done, the public interest requires the Commission to adhere to a policy of neither confirming nor denying any information about the installation, use or retrieval of surveillance devices, beyond that which is required by law.

These representations accordingly first deal with relevant general contextual issues and then return to a consideration of the proposition.

The Parliamentary Inspector's letter dated 6 July 2010 asked for a copy of the retrieval warrant.

As the Commission previously advised, there is no separate retrieval warrant. A warrant issued by a Supreme Court Judge pursuant to section 13(3) of the *Surveillance Devices Act 1998* (WA) (SD Act) authorises the installation, maintenance and retrieval of the relevant device(s).

Accordingly, the warrant issued in this case, (a copy of which was provided to the Parliamentary Inspector on 13 May 2010 and which had previously been disclosed to [Person A] as part of the [redacted] prosecution disclosure) authorised the attachment or installation, maintenance and retrieval of a listening device, optical surveillance device and tracking device (or devices).

Details of Installation or Retrieval

As mentioned in previous correspondence, the Commission has consulted with Federal and State Agencies on this issue. All agencies have the same, consistent position with regard to the non-release of any surveillance device (SD)-related detail (other than that limited information or material which is disclosable and may be given in evidence in judicial or other proceedings).

All Federal and State agencies spoken to about their practices and procedures regarding disclosure of technical surveillance-related information confirmed they do have policies and guidelines on public interest immunity and unit security documentation that address this matter.

These documents are of a highly sensitive nature and reveal planning considerations and practical internal working practices of the agencies concerned.

Indicative reasons why SD information is not revealed include:

(a) the locations in which an audio listening device or other technical surveillance equipment can be secreted are finite and revelation of such information would prejudice present and future operations not only of the Commission, but of all law enforcement agencies (LEAs). (Following a High Court trial in New Zealand in which a witness was compelled to reveal the location where a listening device was installed in premises, that location can no longer be utilised as a place of concealment in future operations).

(b) technical surveillance operations and associated installations, require absolute protection in order to preserve future operations and the safety of police and other LEA officers carrying out this work.

(c) By their nature, all such technical surveillance operations are carried out covertly and public revelation of any matters concerning technology and associated methodologies could only serve to endanger future operations, the safety of officers involved and members of the public.

(d) Law enforcement and other approved agencies may only use listening devices controlled by the provisions of the SD Act or equivalent legislation on the authority of a Judge of the Supreme Court. In practice authority to use listening devices is only given in the case of serious criminal offences. In many law enforcement (eg police or national security agencies) operations in which these methodologies are used, persons of interest generally are often regarded as dangerous and of considerable threat since the consequences to them of offending are high.

(e) From a technical perspective, evidence of the audio coverage given by the device within the premises or place can be given by witnesses without disclosing the location of the technical installation.

Revealing information about or details of technical surveillance equipment, concealments, operating parameters and installation and retrieval could lead to the future discovery of such equipment, and subsequent knowledge by criminals or other subjects of investigation which could compromise future operations by agencies.

Information containing details of technical surveillance equipment and methodologies (or from which they could be inferred) could endanger other facets of similar operations and may:

(a) prejudice present or future operations of a similar nature;

(b) endanger the safety of members of the public; and

(c) compromise the actual use of such devices.

The counter-surveillance industry is growing rapidly in Australia with no regulation and no restriction in the importation of or possession of counter-surveillance equipment. With such people offering their services searching for devices, it follows that methods of placement and concealment have to be of an extremely high standard.

Police and other LEA technical specialists go to extreme lengths and expense to protect electronic surveillance technology and associated methods of operation even within their own ranks. That is certainly the case with the Commission's Operational Support Unit (OSU) whose officers' identities, locations and activities are known to a very limited number of senior Commission officers involved in operational matters. OSU officers utilise methodologies, techniques and technical capabilities which are classified "Highly Protected" and revealed only to other Commission officers with that level of security clearance and who have a need-to-know.

Briefly put, providing surveillance equipment technical details or the supporting methods utilised by the Commission or any information about them, to individuals or bodies that the Commission has investigated, or may in the future investigate, can facilitate those parties (plus others) identifying and subsequently targeting those methodologies that could impact the planning and execution of future Commission operations and the operations of other agencies.

Providing a level of information including dates and surrounding details of surveillance deployments can provide that party (and others) with the ability to identify, examine and learn methods of entry, placement of surveillance equipment and mechanisms by which this is achieved. This then allows parties to prepare "counter methods" to detect, obstruct and harm future surveillance deployments with the resultant affect on the Commission (and other LEAs). Once this information is in the public domain (and not controllable) it can impact on the safety of all government officers who deploy surveillance equipment in future operations.

The position outlined above reflects firm practice across all Australian police forces and other LEAs, supported (for example) by the Australia New Zealand Policing Advisory Agency (ANZPAA) - the National Police Research Unit and Australian Centre for Policing Research (NPRU/ACPR).

Any less rigorous approach taken by this Commission to the disclosure of any of these matters, apart from establishing a precedent which could operate on future operations, would almost certainly affect its reputation and confidence in the integrity of its operational information and impede its future access to classified information, to knowledge of developing capabilities and cooperation with other agencies.

The Commission accepts that, <u>when considered in isolation</u>, the simple proposition as expressed in the draft report, that [Persons A and B] should have the retrieval of the surveillance devices confirmed to them so as to allow their peace of mind, may be thought on the face of it, to be not unreasonable on two grounds. First, some might claim that those individuals subject to such intrusive surveillance have a right to know when that surveillance has ceased. Second, others may also claim that the provision of that information is of finite benefit, in that it would only pertain to those devices deployed for that particular operation, and is inconsequential to anyone else.

The Commission bases its position in regard to not disclosing information about the retrieval of devices on the grounds that there is both no requirement at law for the Commission to make such a disclosure and that to do so would create a precedent with consequences for the conduct of past, current and future Commission operations which may also have further consequences for the broader law enforcement community in Australia.

"Right to Know"

In respect of the first ground, individuals the subject of intrusive surveillance have no statutory right to know whether the devices have been retrieved or not. Indeed, this and other information about the deployment, employment and retrieval of such devices is usually subject to public interest immunity (PII) claims when criminal charges involving surveillance devices go to trial. Typically, such PII claims are allowed and the capacity for the defence to "go behind" the deployment, employment and retrieval of such devices is constrained. The reason for the granting of PII claims in these cases reflects an appropriate balancing of the public interest in ensuring investigations are effective, weighed against the prospect that the administration of justice would be frustrated if the documents or information were withheld.[1]

Whilst not minimising the latter, the public interest in the proper administration of justice affecting the conduct of a particular trial is obviously a very different imperative than an individual's right to privacy (in the sense of being told he or she is not under surveillance or that surveillance has ceased or that devices have been removed).

The Commission notes that despite PII, some information about the use of any relevant surveillance devices and the resultant material gathered is provided to defendants under the prosecution's disclosure obligations. In the case of [Persons A and B], for example, [Person A] had the relevant surveillance device warrants and audio copies of relevant surveillance device product disclosed to him. He was also offered the opportunity to listen to the totality of the SD product obtained from his residence. Such material would enable him to determine that the warrants were in force for a finite and known period.

With regard to any suggested "right-to-know", recent amendments to Surveillance Devices Acts in other Australian jurisdictions have seen the disclosure of information about the retrieval of devices prohibited.

Under section 47(1) of the *Commonwealth Surveillance Devices Act 2004* an individual may object to the disclosure of information in a proceeding[2] on the ground that the information, if disclosed, could reasonably be expected to reveal details of surveillance device technology or methods of installation, use or retrieval of surveillance devices and an order can be granted by a court, tribunal or Royal Commission to prevent publication.

A very similar provision is contained at section 42 of the NSW *Surveillance Devices Act 2007* and section 355(4) of Queensland's *Police Powers and Responsibilities Act 2000* provides for the granting of orders restricting publication of information that could reasonably be expected to reveal details of surveillance device technology, methods of installation, use or retrieval.

The SD Act is currently subject to review and the Commission understands that the inclusion of similar provisions will likely be sought by Western Australia's Police. Further, other jurisdictions are moving to make express provision for the statutory-based protection of much of what now relies on PII applications in the Courts.

Thus, in respect of the "right-to-know" in terms of the retrieval of surveillance devices not only is there no statutory basis for it, but the courts have broadly accepted that such information should be

[1] *Attorney General (NSW)* v *Stuart* (1994) 34 NSWLR 661

[2] Including a proceeding before a court, tribunal or Royal Commission

protected under the PII regime, and there is a move to expressly protect the disclosure of such information by statute. This approach is an important factor that helps to inform the Commission's position in respect of the nondisclosure of information relating to the retrieval of any device or devices from the residence [of Persons A and B].

Disclosure of Whether or not Devices had been Retrieved

As adverted to in its earlier correspondence with you, if the Commission were to disclose the surveillance devices had been retrieved from the residence [of persons A and B] (assuming for present purposes, but not confirming, that they had been) such a disclosure, at the very least would have required qualifications - which would give rise to further operational difficulties. For example, such a disclosure could only pertain to those devices deployed by the Commission for the purposes of the [redacted] investigation. Any such disclosure could not permit any inference to be drawn that the [Persons A and B] either were or weren't the subject of other investigations by the Commission or some other law enforcement agency in the past, for the present or in the future. Beyond that, even apparently innocuous information may give rise to important implications.

For example, the rationale for the general policy of neither confirming nor denying any information about the installation, use or retrieval of surveillance devices, beyond that which is required by law, is vindicated by the way in which the contrary argument has been put in correspondence from the Parliamentary Inspector.

In the letter from the Parliamentary Inspector dated 11 May 2010, it is put that:

> *If such devices are not in place, and there is no current investigation involving* [Person A], *the Commission's continuing silence seems, on the face of it, unjustified and unnecessarily oppressive.* (emphasis added)

That letter continues:

> *I understand that, when there is* a *current investigation ... it would be inappropriate for the Commission to respond ...* (emphasis added)

and

> *It seems to me that if.,... there is no ongoing investigation* of [Person A] *in place, and if no investigation* of *him is in prospect, then ... they are entitled to be reassured that the devices that were previously installed are no longer in place ...* (emphasis added)

Self-evidently, were the Commission to (for example) confirm that there were no devices in place, that would be tantamount to confirming there is no current investigation of the subject individual either in place or in prospect.

No investigative agency would confirm such matters unless there was an operational reason for doing so.

The same point arises out of the fourth paragraph of the letter from the Parliamentary Inspector dated 20 May 2010, where it is said:

> *... There seems to me to be no justification for this in circumstances in which he* [Person A] *is not presently under investigation by the CCC.* (emphasis added)

The Consequences of Disclosure are not Limited

In respect of the second ground, some might suggest that the disclosure of the retrieval could have no meaningful consequence for any other individuals, Commission investigations or other agencies. Such a view is only possible if the issue concerning [Persons A and B] is viewed narrowly.

The Commission is concerned that providing some form of assurance to [Persons A and B] that the surveillance devices were retrieved from their property would create a precedent for the Commission in terms of not only [Persons A and B], but other persons of interest in respect of Operation [redacted] extending to other past, current and future investigations. Whatever caveat is imposed, and or accepted, about any disclosure it is reasonable to expect that should the Commission confirm that any device has (or has not) been removed, [Person A's] associates will be informed of the outcome and may seek similar disclosures from the Commission either now or at some future date. Further, on that basis and on the basis of previous occurrences, it is also reasonable to expect that any disclosure will receive media coverage. Others, who were, or who suspect they were, subject to investigation, could subsequently seek similar disclosures of information about SD. The Commission's standing position is to neither confirm nor deny that an investigation is in train. It applies a similar policy in respect of information about its various investigative capabilities and actions, including particularly its surveillance activities. The consequences of any disclosure concerning the retrieval of the devices from the residence [of Persons A and B] is unlikely to be constrained to just that disclosure. It is more likely than not to lead to expectations that the Commission will confirm the presence or retrieval of other devices in connection with this or other investigations.

The precedent in respect of such disclosures would likely have consequences far beyond the conduct of Commission operations.

The Commission is very conscious of the importance of its relationships with other law enforcement agencies. The Commission is well regarded in terms of its surveillance capabilities, the overall professionalism of its surveillance staff and the high priority it gives to protecting knowledge about its surveillance equipment, tactics, techniques and procedures. The creation of a precedent in relation to this matter would contribute to the overall pressure on other agencies to make similar, and other associated, disclosures. The net effect will be to damage the Commission's reputation.

Any precedent that appears to be a loosening of the Commission's control of information affecting its surveillance capabilities may, through a cumulative effect, weaken that reputation resulting in reduced access to future capabilities. While this may appear to be overstating the consequence of the proposed apparently simple disclosure to [Persons A and B] it is nevertheless representative of the seriousness attached to the protection of such information by the law enforcement surveillance community.

Public Interest versus Private Interests

In addressing the issue of disclosure above, the Commission noted that law enforcement agencies typically seek and are granted PII in connection with the tactics, techniques and procedures used when deploying, employing and retrieving surveillance devices.

The Commission accepts its responsibilities to give appropriate consideration in respect of the requirement for the court to which application for the use of SD is to be made to have regard to, among other factors, the effect on the privacy of any person and the availability of other methods of investigation not involving the use of a surveillance device as required by section 13(2) of the SD Act. I note that section 13(2)(f) also requires that the Judge have regard to the public interest.

When addressing the need to balance public and private interests parliaments and the courts, in certain circumstances, accept the proposition that public interest may outweigh the private interests of individuals. For example:

(a) The *Corruption and Crime Commission Act* (CCC Act) is a law for the peace, order and good government of the State of Western Australia[3] established by the Parliament exercising its "ample and plenary" powers to do so.[4] The Parliament established the Commission with the purpose of improving continuously the integrity of the public sector (section 7A of the CCC Act), implicitly acknowledging its social contract with the people of Western Australia to ensure the peace, order and good government of the State, especially in regard to the delivery of goods and services to the people, protection from harm, and an enduring commitment to the public interest in exchange for the power to enact laws and levy taxes. This protection from harm includes protection from abuses of power by public officers empowered to act in the public interest, that is, the purpose of the CCC Act in regard to improving continuously the integrity of the public sector.

(b) The Parliament, in establishing the Commission, deliberately acted to give the Commission particular powers that reflected:

> *... the willingness of the government and the community to accept the suspension of fundamental civil rights in the interests of detecting forms of serious wrongdoing with the capacity to undermine the integrity of public institutions.*[5]

(c) The issue of weighing public interests against private interests arises in a formal sense for the Commission is at s140 of the CCC Act. This section requires the Commissioner to weigh the public interest when deciding to conduct public examinations by balancing public exposure and awareness against concern for prejudice and privacy infringements. In making this decision the Commissioner has a broad range of authorities on which to draw for guidance. In *Independent Commission Against Corruption v Chaffey (1992)* 30 NSWLR 21 Gleeson CJ asserted that while there was a requirement to weigh a number of competing factors there is:

> *no obligation in* a *commission of inquiry to avoid or minimise publicity in order to protect reputation.*
>
> *... There is* a *fallacy in passing from the premise that the danger to harm to reputation requires the observance of procedural fairness to the conclusion that*

[3] *Dainford Ltd* v *ICAC* (1990) 20 ALD 207

[4] *Union Steamship Co of Australia Ltd* v *King* (1988) 166 CLR 1

[5] Hall, P.M. 2004, Investigating Corruption and Misconduct in Public Office: Commissions of Inquiry - Powers and Procedures, Lawbook Co, Sydney, p.639

> *fairness requires the proceedings be conducted in all respects in such* a *way as to minimise damage to reputation.*[6]

In summary, the Commission's view is that the public interest in it neither confirming nor denying that the surveillance devices were removed from the residence [of Persons A and B] outweighs their private interest in knowing. The Commission has complied with the SD Act. It has no obligation to inform [Persons A and B] whether or not any device has been retrieved. Further, it is the Commission's view that providing such information would create a precedent detrimental to the public interest and that such a disclosure might undermine the capacity of the Commission to deal with subsequent requests for assurances from other persons of interest and that such a disclosure would adversely affect the Commission's standing with other law enforcement agencies. A major consequence of these outcomes would be to adversely affect the capacity of the Commission to conduct its investigations efficiently and effectively.

In this circumstance the Commission's position is best expressed by paraphrasing Gleeson CJ: there is a fallacy in passing from the premise that the danger to harm to the privacy of individuals requires the observance of fairness to the conclusion that fairness requires the public interest be circumvented in all respects in such a way as to minimise damage to privacy.

The Commission considers that it is obliged in the public interest to maintain its policy of "neither confirming nor denying" any information about the installation, use or retrieval of surveillance devices, beyond that which is required by law.

The Commission appreciates the important privacy interest of individuals who are the subject of lawful Commission or other LEA scrutiny which arise here, but on balance in the Commission's view they are outweighed by the very strong public policy considerations explained above.

In short, given the essential need not to erode nor undermine the covert nature of surveillance activities by LEAs, the Commission considers the public interest in strict adherence to the non-disclosure of any information about them beyond that required by law, outweighs the private interests of individuals - and [Persons A and B] should be no exception to that.

As the draft report notes, the Commission adheres to its position that the public interest requires the Commission to maintain its response to [Persons A and B] that it will neither confirm nor deny the retrieval of any surveillance devices from their residence.

For the reasons given above, the Commission does not accept the proposition that adherence to its policy as stated above is either "inappropriate" or that it is capable of an "unnecessarily oppressive" operation, or that it takes a fundamental (if sometimes necessary) inroad into the rights of the individual "further than is justified".

Parliamentary Inspector's Recommendation

The Commission does not agree that there is any requirement to amend the SD Act in the manner proposed in the draft report.

It is not a matter of "competing interests of the CCC (or other agency taking advantage of the provisions of the SD Act)" against "those of persons affected" - that is, those individuals the subject of surveillance devices lawfully installed under a warrant of a Supreme Court Judge.

[6] Ibid pp.652-653

As explained above, it is a question of balancing the public interest in maintaining the operational security and effectiveness of legislatively approved use of surveillance device technology, against the privacy rights of individuals.

As the amendment proposed in the draft report would have significant operational ramifications for all law enforcement agencies utilising surveillance devices under the SD Act, the Commission would strongly support the suggestion made there, that further consultation should be had about any proposal for such amendment.

APPENDIX THREE

TRANSCRIPT OF EVIDENCE TAKEN BEFORE THE JOINT STANDING COMMITTEE ON THE CORRUPTION AND CRIME COMMISSION IN PERTH ON MONDAY 11 OCTOBER 2010

Members

Hon Nick Goiran (Chairman)
Mr John Hyde (Deputy Chairman)
Mr Frank Alban
Hon Matt Benson-Lidholm

STEYTLER, MR CHRISTOPHER DAVID
Parliamentary Inspector of the Corruption and Crime Commission, examined:

ALDER, MR MURRAY COLIN
Assistant to the Parliamentary Inspector of the Corruption and Crime Commission, examined:

The Chairman: Inspector, I would like to move to the second matter for today's purposes. This is the report that you provided on 15 September this year relating to the use of surveillance devices regarding [redacted]. In particular, inspector, the status of the matter is that the committee has had an opportunity to deliberate on one occasion. In essence, we recognise that the matter currently rests with the committee, noting of course, inspector, that at any time you are able to table this report or something similar with the Parliament, should you wish to do so. In particular, inspector, I would like to better understand what I will describe as the difference of opinion between your office and the commission in regard to this matter. The committee is always keen to narrow down what those differences are before it would look to table something in a public forum. Are you able to elaborate on what those differences are?

Mr Steytler: Essentially, the commission takes the view that if there were to be an amendment of the kind that I have recommended, it would do two things: firstly, it would create operational problems for them; and, secondly, it could cause them to lose credibility in the eyes of other agencies, which would be reluctant to share information with them. I have to say that I do not see any substance at all in either of those concerns because, given the very limited scope of the amendment I have proposed, there would be only a right to go to a court to apply for disclosure of whether or not the device had or had not been removed and for an order that it be removed if it had not been removed in circumstances in which it was common cause that a device had in fact been installed pursuant to a warrant that had since expired and in respect of an investigation that was now complete. The kinds of circumstances in which it would apply would be when there was a trial or a hearing, as in this case, whereby it became apparent because the calls were put in

evidence that there had been surveillance and whereby it was apparent that that particular investigation and therefore that particular warrant was concluded. I can understand that the commission would not want anybody to know where the particular device had been installed. For example—just to pull something out of the air—if you put an optical device in a light bulb or a listening device in a flowerpot, you would not necessarily want them to know that that was where they were because that would become known to others and you would not be able to use those places again. Again, I have suggested in my recommendation that when there is an order for the removal of a device, it could be made under terms designed to protect any information of that kind; in other words, the house would have to be vacated and the officers who would go in there would have to be unobserved when they removed the device or devices. I cannot see any difficulty with that.

There is another concern that the commission has; that is to say, if you tell people that there was a device there but it is no longer in operation and it has been removed, they would then have the confidence to know that they were not currently under investigation. They have suggested that that is not a good thing to do with people because they tend to be more honest if they think they are under surveillance about what they have or have not said or have or have not done. Again, that seems to me to be fallacious reasoning. Once somebody gets to the point of applying to court to find out whether or not there is a device there, they are going to be suspicious in any event. Secondly, I do not think it is a legitimate thing to make people think there is a device in their own home when there is not simply to try to encourage them to make admissions that they might not otherwise make. Those are the principal sources of difference between us. Again, so far as losing credibility in the eyes of others, I cannot see why such a limited amendment should cause them to lose any credibility. There would be no information being disclosed of any significance to anyone.

The Chairman: Is there a possibility that a matter such as this could go to a trial stage, yet an investigation that is the subject of a warrant could still be ongoing?

Mr Steytler: There is the possibility that in that event there would be no right to apply to the court because the only time there would be a right to apply is when the investigation that led to the warrant in the first place had been concluded. All you would be doing is applying in respect of that investigation. If some new investigation had commenced, it would not apply.

The Chairman: How would an applicant know whether the investigation was definitively concluded?

Mr Steytler: He might know that if his trial was over in respect of the very charges that had been brought against him, or if the commission, as in this case, for example, had made findings on the matters inquired into and had issued its final report.

The Chairman: Is it possible to apply for a warrant to have a live warrant in place? Some evidence obtained under that warrant has been used for a particular purpose, yet there may be secondary purposes, in which case the warrants are still ongoing?

Mr Steytler: That is possible, but in that event there would be no right to apply because you would not be able to satisfy the condition that all investigations that had based the warrant in the first place had been completed.

Mr J.N. Hyde: There cannot be secondary uses on a warrant. It has to be specific, detailed and finite.

Mr Steytler: Unless they spelt out in the warrant itself that clear purpose.

The Chairman: Again, I am just not clear on how the applicant would know that that was the case in that circumstance.

Mr Steytler: He would not know. Ordinarily he would not know.

The Chairman: Okay; so ordinarily you would not know that.

Mr Steytler: And in that event the application would be refused without giving reasons.

The Chairman: But if it is refused, would the refusal not indicate that there is an ongoing investigation?

Mr Steytler: It may do, though I have dealt with that in the report. That is a shortcoming in what I have suggested and I have raised that in the report. It seems to me that there are a couple of answers to it. One is that it would be a very unusual circumstance. Most warrants relate to a particular investigation and not more than one investigation. I think it is unlikely to arise in practice. Secondly, once you have got to the stage of bringing an application of that kind and in circumstances in which the court is empowered to decline to grant it without giving reasons for any number of reasons: one is in the public interest, that would alert somebody that something is up; another would be that it is not feasible or practical to remove the device for whatever reason. So you would not know; you would suspect that you were under investigation if your application was refused, but you must have suspected anyway by the time you go to court. I accept that that is a potential problem with the amendment that I have drafted. I think it would be a very rare circumstance, but possible.

The Chairman: Would it be equally as rare as the circumstances that we have before us at the moment?

Mr Steytler: Yes, I think that is a fair comment.

Mr J.N. Hyde: We are only dealing with this because in the CCC's own investigation they have revealed that the matter was finished with in court publicly. I cannot see, feasibly, how there could be another situation in which somebody would have empirical evidence that they had been bugged.

The Chairman: Are we saying then that it was a mistake for that to be disclosed in a public forum?

Mr J.N. Hyde: No. The whole thing about people saying, "You have got to have your day in court"—well to have your day in court evidence has got to be produced. The system works, so to me there is therefore no obstacle to having full transparency once it has gone to court and been revealed that a bug was in place.

The Chairman: Although you revealed there was a bug in place, is it necessary to go that one step further and say that the investigation is concluded?

Mr J.N. Hyde: I think there is in the interest of transparency and making people understand about how very limited TIs and SDs actually are. Because I think [redacted] in particular, not so much [redacted], has got away with creating a fear that people are being bugged for seven years at a time and I think perhaps [redacted], more so, is perhaps scared, as are others. They are, and I think in the interests of transparency this is saying to the community, "Look, it is very rare for a warrant

to be extended once. If it is actually extended twice or three times you are only looking at a time period of eight months or nine months; it is not a matter of years."

Mr Steytler: The other thing, I think, that might be relevant here is that, as I have said, this kind of situation is only going to arise when there is evidence given of intercepted conversations or video surveillance is actually produced in court or in hearing some kind. That is unlikely to happen until the end of the investigation, until the investigation has been completed. So as I have said, while it is possible, I would not doubt that, it is rare. The other consideration is that one has to weigh the possibility that it might deepen an already held suspicion against the effects of someone knowing that there is a device in their home or thinking that there might be in circumstances in which the only investigation against them has been completed, and in which they are not under suspicion for anything and have not done anything. One need only imagine how intrusive it must feel to know that there might be surveillance device in your home—a camera, a listening device—and you can be told, "Well they cannot activate it without a warrant", but would you necessarily believe that? I am not sure you would. In this case, [redacted] did not believe that and I suspect that they still do not. One cannot take individual instances as being definitive of anything, but most people who would know that there is a surveillance device in their home somewhere, even inactive, would feel uncomfortable about it, I think. We got a sense, even the other day, talking to [redacted], about how intrusive this kind of surveillance really is and what kind of an effect has on people. I think that is something that needs to be weighed and balanced as well. I understand that investigating agencies do not weigh that in a balance, but I think perhaps they should.

Mr J.N. Hyde: Can I add in one other scenario that perhaps has not been discussed? Taking the issue of [redacted] or somebody who was doing something illegal out of a vehicle, we will say clearly there was a bug in his vehicle—or the New South Wales royal commission, with the coppers taking the cash in the car. The proceeds of crime, the $200 000 Maserati or Rolls Royce, could be taken and flogged. If you are buying that from an auction or whatever, you would quite rightly want to say, "I am getting a vehicle, you can tell me that bug is no longer in there, surely." Under the current legislation the CCC would not be able to say, "Of course we have taken the bug out", but under this you would. I do not know if that is a little bit left of field, but to me that seems relevant.

The Chairman: As I understood it, the proposal here is that someone has to make application to the Supreme Court.

Mr Steytler: That is right.

Mr J.N. Hyde: Well the police could do that. If it is proceeds of crime and the difference is between getting 200 grand for a Maserati or having Rob Johnson squelch it and get nothing, I think a short trip to the Supreme Court might be worthwhile.

Mr Steytler: Of course the commission does not need to go to court. It does not need to compel the person to go to court; the commission could just tell them itself. There is nothing that prevents it from doing so. The only reason I put in the ability to go to court is because it has made quite plain to me that it will never tell unless it is compelled to.

The Chairman Yes, as I understand it, that is right. There is not a legislative hurdle for the commissioner in disclosing, it is more a matter of concern for policy, procedure, precedent and convention that prohibits it from occurring at the moment.

Mr J.N. Hyde: Clearly your advice as our parliamentary inspector is that it should be made public—that there should be an avenue in exceptional circumstances if the CCC determined not to confirm —

Mr Steytler: Yes, that is my position. I recognise the weight of what the chairman has said, but it seems to me that the other interests are greater than that and it also seems to me that is likely to be a situation of very limited application.

The Chairman: Inspector, if the committee was minded to present a report to the Parliament, are there elements of this particular report that you provided to us, dated 15 September 2010, that you would have any reservation in being provided to the Parliament? I note that in particular there is the suggestion that the commissioner of the CCC says it is inappropriate for the schedules other than schedule 8, which of course was the CCC's submission—the rest ought not be provided. My initial feeling is that I have some sympathy for that, but I just want to get your view.

Mr Steytler: That would be my recommendation, that the report be provided with only schedule 8. It would mean that Parliament will not have all the information that you might want, but I think that the body of the report is designed to give Parliament sufficient information to make what is essentially a policy decision.

The Chairman: In that same vein, inspector, the portion of today's closed hearing that deals with this particular issue: would you have any reservations in it being provided to the Parliament?

Mr Steytler: No.

The Chairman: Members, do we have any other questions on this? Inspector, any other comments?

Mr Steytler: No, I am fine.

The Chairman: Then, inspector, that concludes the two major items of business. Are there any other matters that you want to discuss with the committee this afternoon.