



## Office of the Parliamentary Crime and Corruption Commissioner

Parliament House  
George Street  
Brisbane Qld 4000  
Ph: 07 3553 6652 Fax: 07 3553 6654  
pcc.commissioner@parliament.qld.gov.au  
www.parliament.qld.gov.au/pccc

Your Reference: qA19745

10 August 2020

Committee Secretary  
Parliamentary Crime and Corruption Committee  
Parliament House  
George Street  
BRISBANE QLD 4000

By email: [pccc@parliament.qld.gov.au](mailto:pccc@parliament.qld.gov.au)

Dear Committee Secretary,

### **Re: Five-year review of the Crime and Corruption Commission's activities**

I refer to the 1 June 2020 letter from the Parliamentary Crime and Corruption Committee (the Committee) inviting me to make a submission to the Committee's five-year review of the activities of the Crime and Corruption Commission (CCC). The Committee advised that it will examine the CCC's performance, jurisdiction, responsibilities, functions and powers. Other matters to be examined include oversight arrangements, the roles of the responsible Minister, the Committee, the Parliamentary Crime and Corruption Commissioner and the Public Interest Monitor.

Below I have identified particular issues which have arisen during the performance of my functions.

### **Oversight Arrangements**

#### **1. Continuity of Committee membership**

The continuity of the Committee membership is an issue which has concerned me for some time. The relevant provisions are s.300 and s.301 of the *Crime and Corruption Act 2001* (the Act). Section 301 ensures the continuity of Committee membership after the dissolution of the Legislative Assembly. A Committee member remains a member until the member resigns, dies or the Electoral Commission is notified that the member has not been re-elected. That is a significant exception to the usual rules applying to Portfolio Committees. Over my time there have been significant changes to the Committee membership, for example between late 2017 and early 2018. It is preferable that there be the appointment of no more than four new Committee members at any one time or in a short space of time – subject to their re-election. This would ensure a level of continuity of Committee membership and shared knowledge which would enhance the Committee's oversight of the CCC.

#### **2. Parliamentary Commissioner's own initiative investigations under s.314(4)**

Presently, s.314(4)(a) of the Act provides that the Parliamentary Commissioner may only investigate on their own initiative a matter that relates to conduct of a commission officer that involves or may involve *corrupt conduct* - as defined in s.15 of the Act. Corrupt conduct under s.15(1)(a) is conduct that adversely affects, or could adversely affect, directly or indirectly, the performance of functions or the exercise of powers of a unit of public administration (UPA) or a person holding an appointment in a UPA.

Section 20(2)(a) states that the CCC is not a UPA and a CCC officer does not hold an appointment in a UPA (unless the officer is on secondment from a UPA). Purely internal conduct of a CCC officer cannot be *corrupt conduct*. The only conduct of a CCC officer which could be the subject of an own initiative investigation is conduct which adversely affects the performance of functions or the exercise of powers of a UPA or a person holding an appointment in a UPA. This significantly limits the Parliamentary Commissioner's own initiative investigative jurisdiction.

To address a similar lacuna in the s.329 definition of *improper conduct*, s.329(4)(c) was inserted by the 1 July 2014 amendments. Section 329(4)(c) states that *improper conduct* includes conduct of a CCC officer "*that would, if the person were an officer in a unit of public administration, be corrupt conduct.*" Since that amendment, the equivalent of corrupt conduct suspected on the part of a CCC officer is *improper conduct* which must be notified to the Committee and the Parliamentary Commissioner.

Section 314 of the Act could be similarly amended to include conduct that would be corrupt conduct if the CCC officer were an officer in a UPA. Otherwise, the Parliamentary Commissioner's own initiative jurisdiction under s.314(4) is too restricted. The section might be amended as follows:

- (4) *The parliamentary commissioner also has the function to investigate on his or her own initiative a matter mentioned in subsection (2)(b) or (c), or a matter notified to the parliamentary commissioner under section 329, if—*
- (a) *the matter relates to conduct of a commission officer that involves or may involve corrupt conduct **or conduct that would, if the person were an officer in a unit of public administration, be corrupt conduct**; and*
  - (b) *the parliamentary commissioner is satisfied, on reasonable grounds—*
    - (i) *the commission has not adequately dealt with the matter; or*
    - (ii) *the commission may not adequately deal with the matter; or*
    - (iii) *it is in the public interest.*

## Surveillance Device Warrants

### 3. Use of surveillance device warrants in Corruption Investigations

The Committee may wish to consider clarifying the legislative basis for the CCC's use of surveillance device warrants under the *Police Powers and Responsibilities Act 2000* (PPRA) for the purpose of corruption investigations. You may recall this issue was previously explored with the CCC.

Some uncertainty is created by s.325(4) of the PPRA which provides:

- (4) *A function conferred under this chapter [Chapter 13 – Surveillance Devices] in relation to the activities of the CCC is only conferred for the purpose of a function conferred on the CCC under the Crime and Corruption Act 2001 relating to major crime as defined under that Act. (my underlining)*

This suggests that that the CCC can only use PPRA surveillance device warrants for the purpose of its major crime function. However, the example beneath s.255(5) of the Act conflicts with s.325(4) of the PPRA to some extent. Section 255(5) includes a note:

*A police officer seconded to the commission may exercise the powers of a police officer under the Police Powers and Responsibilities Act 2000 for an investigation of alleged corruption involving a relevant offence as defined in section 323 of that Act. (my underlining)*

So, for a corruption investigation, a CCC officer who is not a police officer cannot apply for a PPRA surveillance device warrant. However a senior police officer seconded to the CCC can. There would not seem to be any valid reason for that distinction.

The Committee may wish to consider reviewing s.325(4) of the PPRA. If Parliament intended that the CCC be able to obtain surveillance device warrants under the PPRA for both its corruption and major crime investigations, s.325(4) should be amended to remove its present limitation to functions relating to major crime. On the other hand, if it was Parliament's intention to restrict the CCC's use of PPRA surveillance device warrant powers only to major crime investigations, s.255(5) requires amendment.

#### **4. Manner in which surveillance device warrants are extended**

This is also a matter previously raised with the Committee. Section 333 of the PPRA deals with applications for the extension and variation of surveillance device warrants, that is optical, listening and tracking devices. Section 333(5) states that if the judge or magistrate grants the application, the judge or magistrate must write the new expiry date or the other varied term on the original warrant. Those varied terms can be lengthy.

This Office has historically held reservations about extending surveillance device warrants in this manner. The handwritten amendments and variations of some judges can be difficult to decipher. The warrant conditions are often quite detailed and complex. They must be understood and strictly followed by monitoring staff and any technician installing the devices. It is preferable for a new warrant to be issued rather than seeking an extension to an existing warrant.

Concerns were first raised about this procedure as far back as 25 February 2005 when the then Parliamentary Crime and Misconduct Commissioner, Mr Alan MacSporran QC, made a submission in relation to the proposed cross-border law enforcement legislation amendments to the PPRA. Mr MacSporran observed that:

...if a Judge grants the application, the Judge must endorse the new expiry date or other varied term on the original warrant. That is different to the present situation where an entirely new warrant is required for each extension. I am not convinced that endorsing the new expiry date or varied term on the original warrant is the most satisfactory approach. I would consider a fresh warrant to be a neater method together with a requirement that all earlier warrants are maintained and kept on the same file. This is possibly not a significant matter but in my view allowing the original warrant to be endorsed with variations could lead to some confusion as to what the warrant at any given point in time actually authorises. It is a much neater result to have all warrants kept but fresh dated warrants which easily indicate what powers the warrant authorises at any given point in time.

In a letter to this Office dated 24 June 2020 Mr MacSporran stated that, as a matter of principle, the CCC agrees that the method for extending warrants under s.333 of the PPRA raises issues. The CCC supports a legislative change to this provision but any change would be subject to external legislative consideration (such as cross-border recognition of warrants) and consultation with relevant stakeholders.<sup>1</sup>

It should be noted that there is no mechanism for extending telecommunications interception warrants obtained under the *Telecommunications (Interception and Access) Act 1979 (Cth)*. New warrants must be obtained each time. Obtaining a fresh warrant rather than extending an existing warrant appears to be the best practice.

#### **5. Applications for extension and/or variation of surveillance device warrants**

Section 333(1) of the PPRA states that a senior officer of an agency may apply, at any time before the expiry of the warrant, for an extension or variation of the warrant. The application must be made by the officer to whom the original warrant was issued. This requirement has caused difficulties for the

---

<sup>1</sup> There are similar provisions requiring the judge or magistrate to write the new expiry date or the other varied term on the original warrant, in most other States' surveillance device legislation: see s.19(5) of the *Surveillance Devices Act 2004 (Cth)*, s.22(5) of the *Surveillance Devices Act 2007 (NSW)*, s.20(5) of the *Surveillance Devices Act 1999 (Vic)*, s.14(5) of the *Police Powers (Surveillance Devices) Act 2006 (Tas)*, s.19(3) of the *Surveillance Devices Act 1998 (WA)* and s.24(5) of the *Surveillance Devices Act 2007 (NT)*. There is no equivalent provision in the *Surveillance Devices Act 2016 (SA)*.

CCC where the officer to whom the original warrant was issued is unavailable or has left the CCC. It is then necessary for a different applicant to seek the revocation of the previous warrants and the issue of new warrants in similar terms for a further operational period.

The equivalent provisions in the *Crime and Corruption Act* and in each of the other States, the Northern Territory and the Commonwealth do not require the application for extension or variation of a surveillance device warrant to be made by the officer to whom the original warrant was issued.<sup>2</sup> Consideration should be given to amending s.333(1) of the PPRA to permit an application for an extension or variation of a surveillance device warrant to be made by an authorised CCC officer.

## 6. Judge required to provide notice of revocation of surveillance device warrant

Section 334(3) of the PPRA states that a judge or magistrate who revokes a warrant must cause notice of the revocation to be given to the chief executive officer of the law enforcement agency. It is unusual for a legislative provision to require a judge to perform such a role. This issue was discussed in the recent Report on my inspection of the CCC's surveillance device warrant records. Mr MacSporran agreed in principle with this observation in relation to the role of the judge or magistrate.

The New South Wales and Northern Territory Acts state that if a Judge revokes a warrant on the application of a law enforcement officer, the Judge is taken to have given notice to the chief executive officer of the law enforcement agency when the warrant is revoked. That is a more common provision rather than requiring the Judge to notify the chief executive officer of a law enforcement agency.

However, it would be preferable for a formal revocation notice to be prepared by the CCC and signed by the revoking Judge rather than rely on the applicant officer communicating the revocation to the chief executive officer. Mr MacSporran advised that the CCC's usual practice is to prepare a draft notice of a revocation to be signed by the judge as part of the revocation process. In my view, this procedure should be required by the PPRA.

## 7. Surveillance device warrants in the office of a practising lawyer

Section 330(3) of the PPRA states that, "*The judge or magistrate may issue a warrant for the use of a surveillance device in the office of a practising lawyer only if the application for the warrant relates to the lawyer's involvement in a relevant offence.*" This prevents the use of listening devices in a target's lawyer's office to monitor the target's legal strategies and other conversations attracting legal professional privilege. This is a worthwhile provision but it may not go far enough.

Many legal practitioners use their mobile telephones to provide legal advice from home or while driving their vehicles (hands-free). These situations would not be covered by s.330(3) as presently worded. Perhaps the section could be reworded to the effect that "*The judge or magistrate may issue a warrant for the use of a surveillance device in relation to a practising lawyer only if the application for the warrant relates to the lawyer's involvement in a relevant offence.*"

<sup>2</sup> Pursuant to s.127(3) of the *Crime and Corruption Act* a surveillance warrant may be extended "*on an application*". Section 121(2) states that the application must be made by an authorised commission officer with the Chairperson's approval. It need not be made by the officer to whom the previous warrant was issued.

Section 24(1) of the *Surveillance Devices Act 2007 (NT)* permits an application for an extension or variation to be made by the "*A law enforcement officer or an ICAC officer to whom a surveillance device warrant has been issued (or another person on the officer's behalf)...*"

Section 19(1) of the *Surveillance Devices Act 2004 (Cth)*, s.22(1) of the *Surveillance Devices Act 2007 (NSW)*, s.20(1) of the *Surveillance Devices Act 1999 (Vic)* and s.14(1) of the *Police Powers (Surveillance Devices) Act 2006 (Tas)* all permit an application for extension or variation of a surveillance device warrant to be made by "*A law enforcement officer to whom a surveillance device warrant has been issued (or another person on his or her behalf)...*"

Section 19(1) of the *Surveillance Devices Act 1998 (WA)* states that a person who is authorised to apply for a surveillance device warrant may apply to a court for an extension of the period that a warrant is to be in force.

Section 17(2) of the *Surveillance Devices Act 2016 (SA)* states that "*An officer of an investigating agency may, for the purposes of an investigation by the agency, apply to a judge for the variation or renewal of a surveillance device (general) warrant.*"

## Telecommunications Interception Warrants and Surveillance Device Warrants

### 8. Requirement that Public Interest Monitor be notified of breaches of warrant conditions

Telecommunications interception warrants and surveillance device warrants are issued to the CCC subject to a number of standard and, on occasions, specific individual conditions. When the breach of a warrant condition also constitutes suspected *improper conduct* as defined in s.329(4) of the Act, the CCC must notify the Committee and the Parliamentary Commissioner pursuant to s.329(1). (Legislative provisions limit, to some extent, the details the CCC can provide to the Committee concerning telecommunications interception warrants<sup>3</sup> but breaches of telecommunications interception warrant conditions are reported to me in detail in my capacity as Inspecting Entity under the *Telecommunications Interception Act 2009*.)

There is no legislative requirement for the CCC (or indeed any interception agency or law enforcement agency) to report breaches of conditions of telecommunications interception or surveillance device warrants to the issuing authority or to the Public Interest Monitor (PIM).

Nevertheless, as you know, following an exchange of recent communication, the CCC will inform the PIM of such breaches.


In my view, the surest way to ensure breaches of warrants conditions are properly considered is to insert into the relevant legislation, a requirement that the PIM or issuing authority immediately be advised of any breach of a warrant condition. Section 331(1) of the PPRA sets out all the details that a surveillance device warrant must contain. Section 49 of the *Telecommunications (Interception and Access) Act 1979 (Cth)* sets out the form and content of telecommunications interception warrants. These sections should require that every warrant include a condition to the effect that any breach of a warrant condition must immediately be reported to the PIM or the issuing authority.

I acknowledge that an officer or an agency might fail to report a breach of another warrant condition and that this would also constitute a breach of the proposed condition itself. In my view that would likely place any evidence obtained in breach of the first condition in danger of being excluded at trial – a very real disincentive to not reporting the first breach.

#### Important note

A number of these issues concern the exercise of the CCC's powers under the PPRA and the *Telecommunications (Interception and Access) Act 1979 (Cth)*. The relevant provisions of the PPRA were inserted by the *Cross-Border Law Enforcement Legislation Amendment Act 2005*. That Act adopted the provisions of model laws for a national set of powers for cross-border criminal investigations. Any amendment of these provisions must take into account the need to maintain cross-border recognition of Queensland's exercise of the powers. Amendments to the Commonwealth telecommunications interception legislation are, of course, a matter for the Commonwealth.

Yours faithfully



Karen Carmody  
**Parliamentary Crime and  
Corruption Commissioner**

---

<sup>3</sup> See s.63 of the *Telecommunications (Interception and Access) Act 1979 (Cth)*.