CORRUPTION AND CRIME COMMISSION OF WESTERN AUSTRALIA

Submission to the Senate Legal and Constitutional Legislation Committee on the Telecommunications (Interception) Amendment Bill 2006 (Cth)

21 March 2006

SUMMARY

The Corruption and Crime Commission of Western Australia (the Commission) supports the amendments to the *Telecommunications (Interception) Act 1979* (TI Act) proposed in the Telecommunications (Interception) Amendment Bill 2006 (the Bill).

The Commission supports the proposed new mechanisms for access to information and interception, as well as the proposed preconditions for access and interception and the other checks and balances in the Bill.

In this submission the Commission comments on two particular aspects of the Bill, being the proposals to enable:

- interception of communications of a person known to communicate with a person of interest (B-party interception); and
- interception of communications from an identified telecommunications device such as a mobile phone handset (equipment-based interception).

In relation to B-party interception, the Commission anticipates the Committee may be concerned about privacy implications. However, the scope for B-party interception is limited by the preconditions in the proposed subsection 46(3) of the TI Act (Schedule 2 clause 9 of the Bill)[1]. The Commission envisages that with these preconditions in place, there would be a limited number of situations in which B-party interception would be available.

In this submission the Commission gives the following examples of the circumstances in which B-party interception would assist its investigations:

[1] Schedule 2, clause 9, paragraph (3) of the Bill provides that:

"a Judge or nominated AAT member must not issue a warrant (to intercept a B-party's service) unless he or she is satisfied that:

(a) the agency has exhausted all other practicable methods of identifying the telecommunications services used, or likely to be used, by the person involved in the offence or offences referred to in paragraph (1)(d); or

(b) interception of communications made to or from a telecommunications service used or likely to be used by that person would not otherwise be possible."

- Where the suspected offender does not subscribe to a service, subscribes in false names or uses public telephones.

- Where there is information indicating a suspected offender uses a covert telephone service as well as traceable services but there is insufficient information to identify the covert service.

- Where there is information indicating criminal conduct within a group but insufficient information to establish the identity of the persons committing the offences.

- Where a prisoner is involved (prisoners cannot generally be linked to a service) and there is information that the prisoner is involved in criminal activity facilitated by an unidentified public officer.

In relation to equipment-based interception, the Commission regularly encounters persons of interest who are aware of investigative methodology and who use more than one SIM card to avoid interception. The ability to intercept communications from or to a mobile handset would have greatly assisted the effectiveness of Commission investigations in the past and would continue to do so in future.

THE COMMISSION'S CURRENT INVESTIGATIVE FUNCTION

The Commission commenced on 1 January 2004 and received its interception powers under the TI Act on 24 March 2004.

The Commission is established by the *Corruption and Crime Commission Act 2003* (WA) (the CCC Act). One of its functions is to investigate allegations of misconduct by Western Australian public officers, including police officers. The scope of "misconduct" under the CCC Act extends to the most serious criminal offences, such as those that constitute class 1 and class 2 offences under the TI Act, including the class 2 offences of drug trafficking, serious fraud, bribery or corruption of or by an officer of the State, money or property laundering, dealing in child pornography and organised theft.

The Commission is a declared agency under the TI Act. It therefore can use its interception powers to investigate a public officer's suspected involvement in the commission of a class 1 or class 2 offence. Through a combination of its jurisdiction under the CCC Act and its TI Act powers, the Commission can apply for an interception warrant to assist an investigation into whether a particular public officer has committed a class 1 or class 2 offence, or is committing or is likely to commit a class 1 or class 2 offence.

A Commission investigation into the suspected criminal activities of a public officer may encompass the activities of a person who is not a public officer but who is suspected to be criminally involved with the public officer.

Since it commenced on 1 January 2004 the Commission has already investigated some matters in which one or more public officers have been suspected of being criminally involved with persons who are not public officers.

THE COMMISSION'S POWER TO INVESTIGATE ORGANISED CRIME

At present the Commission does not have powers to itself investigate organised crime unless, in a particular case, it suspects that a public officer is involved.

In a report to the Joint Standing Committee on the Corruption and Crime Commission (the JSC) on 7 December 2005, which the JSC has published, the Commission recommended that the scope of the Commission's investigative function be extended to encompass the investigation of organised crime in joint task force arrangements with Western Australia Police and other law enforcement agencies, irrespective of whether a public officer is involved.

The JSC is currently conducting an inquiry in relation to this and other recommendations made in the Commission's December 2005 Report. It is therefore possible that the Western Australian Parliament will give the Commission the power to investigate when it suspects organised crime has been committed, is being committed or is likely to be committed, by persons who are not public officers.

The Commission is therefore interested in any proposed measures that will enhance its ability to investigate not only the links between organised crime and public officers but also to investigate suspected organised crime where it is not immediately apparent that a public officer is involved.

THE NEED FOR B-PARTY INTERCEPTION

Based on its investigative experience so far the Commission predicts that it is only a matter of time before it is faced with circumstances of the type that could be addressed by B-party interception. If the TI Act is not amended to allow B-party interception, the Commission anticipates that some investigations will be protracted and costly and will not capture key evidentiary material.

Police officers and participants in organised crime are generally aware of interception capability and are more sophisticated in their criminal methodology. B-party interception is likely to be particularly valuable in investigations involving these types of suspected offenders who may go to considerable lengths to do what they believe will prevent or restrict interception and other electronic surveillance.

Call charge records and subscriber data cannot stand alone as evidence. Call content has much greater evidentiary and investigative value. The content of a call may contain key evidentiary material about a person's voice, the nature and timing of apparent stressors or the person's actual or anticipated movements or contacts with other persons, all communicated to an unwitting B-party. Call content can provide further investigative opportunities, such as a basis for physical surveillance or other forms of electronic surveillance.

In some situations, a call to a B-party may be the only opportunity the investigative agency has to capture direct evidence in relation to an offence, whether inculpatory or exculpatory.

The Commission can give a number of examples of scenarios it expects to encounter where B-party interception would assist the investigation.

Where the suspected offender does not subscribe to a service, subscribes in false names or uses public telephones

The Commission may have grounds to suspect an individual is committing an offence but may not be able to identify which services the person is likely to be using through a normal non-warrant request for subscriber details under the *Telecommunications Act*. The suspected person may not subscribe to a service or may have subscribed

in one or more false names, such as through a pre-paid SIM card activated over the phone using false credit card details, or a SIM card purchased over the counter at an outlet that does not request proof of identity.

The Commission's intelligence may indicate that the suspected person has a close relationship with a particular relative (the B-party) who is not suspected to be criminally involved with the suspected person but who may be vulnerable as a conduit for the suspected person's communications or criminal dealings. For example, the Commission may believe the B-party's premises are being used as a drop-off point for messages.

Call charge records may indicate frequent telephone communications between the relative's number and one or more public telephone services.

B-party interception of the relative's service may give the Commission information about the suspected person's whereabouts, movements, patterns of behaviour, premises visited, associates and any communications or hand-overs made at or near the B-party's premises.

If the suspected person has subscribed to a service in a false name, the call associated data obtained during interception would enable the Commission to link the suspect to the false name.

Further, if a pattern of use of particular public telephones emerged, such as use of telephones within a particular area, this may indicate that the suspected person is likely to use these telephones to conduct criminal activities. This in turn would enable the Commission to do a non-warrant search of call data from these telephones to search for links with suspected criminal figures and patterns of communication.

In relation to privacy considerations, interception of the B-party's service is preferable to any interception of a public telephone, even if there is information indicating that the suspected person is likely to use one or more particular public telephones.

Where there is information indicating a suspected offender uses a covert or secret telephone service as well as traceable services but there is insufficient information to identify the secret service

Commission investigators who have come from other law enforcement agencies have had experience with sophisticated individuals who subscribe to services in their own name to create an impression of propriety but who also subscribe to other services in one or more false names (secret services). They use the normal services to conduct an apparently law-abiding life and use the secret services to conduct criminal activities.

In these circumstances the Commission would intercept the known services, which may not provide any information about criminal activity. However, if the Commission suspects a secret service is also being used but cannot identify it, the Commission could intercept a B-party's service, provided the Commission had information indicating the suspected person is likely to contact the B-party using the secret service.

The B-party interception would provide data about the secret service, such as the service number, which would lead to other investigative opportunities including the

possibility of intercepting the suspected person's secret service instead of the B-party's service.

Where there is information indicating criminal conduct within a group but insufficient information to establish the identity of the persons committing the offences

The Commission may have grounds to suspect that a number of persons within a group of public officers are committing offences based on the evidence of a criminal informant who has access to the group. An informant may have alerted the Commission to the conduct but without precise details of who is involved.

The Commission may have information indicating that a number of persons within the group have done a number of things but not evidence to identify the particular persons involved. So, even though the Commission may have information indicating criminal conduct it would not have sufficient information to apply for a warrant to intercept the services of any particular individual.

Examples of this would be drug trafficking or money laundering activity amongst a group of police officers, or officers in the government's car licensing department being involved in a car rebirthing syndicate.

It may not be appropriate, for various operational reasons, to ask the informant to consent to interception of his service. Interception of the informant's service under warrant could yield information indicating which individuals are involved. The services of the identified individuals could then be intercepted under the usual form of service or named person warrant.

Even if the Commission has a person (a B-Party) who consents to their services being intercepted, such as an undercover operative or a witness or complainant who has been solicited or threatened, it would still be necessary to obtain a B-party interception warrant as the person communicating to the B-party (the suspected person) would not be consenting to any interception.

The B-party mechanism would therefore allow the Commission to intercept the service of a consenting undercover operative, witness or complainant. Privacy should be less of a concern in this type of cases, as one party to the communications will have consented.

Where a prisoner is involved and there is information that the prisoner is involved in criminal activity, facilitated by an unidentified public officer

The Commission may have information that a prisoner is involved in supplying dugs within a prison, facilitated by a public officer who it has not been able to identify.

It is known that prisoners unlawfully access mobile phones and pass them around inside prisons. The prisoner would not have a service subscribed to him or her and may not use a service or may use various services intermittently that cannot be linked to the prisoner through call charge records or other call data.

The Commission may not have any reason to suspect the B-party (such as the prisoner's girlfriend, boyfriend or spouse, or some other person unwittingly caught up in the prisoner's network, such as a prison tutor) is criminally involved in the supply into or distribution within the prison. However, interception of the B-party's service may provide information that could assist to identify the prisoner's associates inside

and outside the prison and any public officers involved. B-party interception could also provide information about the types of drugs involved, the method and extent of distribution and how the prisoner is paid for the drugs.

EQUIPMENT-BASED INTERCEPTION

Although the Commission is a relatively new agency and has been exercising its intercept powers for only two years, the Commission has investigated matters in which equipment-based access interception would have assisted the investigations.

The Commission regularly encounters persons of interest who are aware of investigative methodology and who use more than one SIM card to avoid interception and disrupt investigators' attempts to identify criminal conduct.

These persons may frequently change SIM cards in their mobile handsets or swap SIM cards around with associates. This diminishes the effectiveness of the interception methods currently available as it takes time and resources to repeatedly identify the service a person is using or likely to be using.

Even with a named person warrant in place the Commission must identify the new mobile service being used and follow an internal process to justify a senior officer approving any request that the carrier intercept a new service under the named person warrant.

This constant changing of SIM cards slows down the investigative process significantly as it requires more requests to the carrier for call associated data, more analysis of the changing circumstances and repeated preparation of written material to justify an internal application to intercept a new service under the named person warrant. In this time vital evidentiary material, including evidence of crucial criminal events, may be missed.

The Commission's view is that the ability to intercept any communications from or to an identified piece of equipment, such as a mobile handset, would greatly assist the effectiveness of Commission investigations in the circumstances described above, which the Commission has already encountered.

CONCLUSION

The Commission would be happy to address any questions the Committee may have about this submission or provide any further information that may be required.