

March, 2006

Mr. Jonathon Curtis
Committee Secretary
Legal and Constitutional Senate Committee
Parliament House,
Barton, ACT

Dear Mr Curtis,

Re: Inquiry into the provisions of the Telecommunications (Interception) Amendment Bill 2006.

Thank you for the opportunity to make a submission to the Parliamentary inquiry.

South Australia Police are pleased to see that this important legislation is being examined with a view to being updated following the Blunn review recommendations. It is imperative that interception legislation keeps pace with criminal methodologies, and endeavours on a national basis to keep a contemporary suite of options for law enforcement are supported. I provide the following submission concerning the proposed amendments.

- **Establish a regime to govern access to stored communications held by a telecommunications carrier.**

It is difficult to predict the impact of the reporting requirements of the proposed stored communications regime. The number of occasions that these provisions will be used is not expected to be excessive at this time but the potential growth in this area of investigation could see an increased administrative burden placed upon our agency by the reporting requirements.

It appears that the intermediate warrant level that has been drafted to place a standard somewhere between a Section 282 Telecommunications Act request and a Telecommunications (Interception) Act warrant has created a very proscriptive and detailed level of reporting which has parallels with the requirements for Telecommunications (Interception) Act warrants.

The importance of privacy of individuals being protected is recognised and the need for a defined stored communications regime is also accepted, however a certification process rather than a warrant process would have been preferred. The inspection of records in possession of South Australia Police by the Police Complaints Authority has always been facilitated and it is preferred that the Commonwealth Ombudsman make arrangements so that Stored Communications records are inspected by our State inspecting authority at the same time as other inspections.

An assessment of the impact upon agencies of reporting under this regime and the arrangements with the Commonwealth Ombudsman should be evaluated at future 'milestone dates' to measure the efficiency and effectiveness of the reporting regime.

- **Enable the interception of communications of a person known to communicate with a person of interest.**

Substantial media interest has been generated by this proposal and is seen as an essential tool if law enforcement is to effectively seek to intervene in cases of extortion, and unlawful threats.

Experiences in South Australia have shown that the current interception framework has not been able to assist in cases where the telecommunications service of the suspected criminal cannot be identified. A recent example of a case in which this provision would assist was that of a person being threatened and extorted by a member of an organised criminal group. In this case the ability of law enforcement to intercept communication services of the intended victim would have assisted to identify the culprit and capture incriminating communications.

This proposal is supported.

- **Enable interception of communications from an identified telecommunications device such as a mobile phone handset**

Experience has shown that criminals are regularly swapping SIM cards and making it very difficult for law enforcement to identify services being used for criminal purposes.

This proposal is supported.

- **Remove the distinction between class 1 and class 2 offences for which telecommunications interception powers are available to law enforcement agencies**

Any process of simplifying the description of offences for which warrants can be obtained is supported, and further steps to simplify the description of Class 2 offences would be welcomed. By way of illustration, rape is not an offence for which an

interception warrant can be issued unless it can be shown that the particular conduct in the case constituting the offence involved serious personal injury or serious risk of serious personal injury.

It is submitted that the qualification of conduct to satisfy class 2 offences descriptions should be removed in favour of a regime where serious offences are captured by offences being punishable by 7 years or more. Another class of offence to capture corruption, child pornography and significant offending that does not carry a 7 year term of imprisonment should also be considered.

- **Remove the Telecommunications Interception Remote Authority Connection (TIRAC) function currently exercised by the Australian Federal Police and transfer the associated warrant register function to the Department administering the legislation**

This proposal is supported, the removal of the TIRAC function will remove a number of administrative matters from the process of activating a warrant and also the process of producing evidentiary certificates by the Australian Federal Police at any subsequent court hearings.

These submissions were prepared by Detective Senior Sergeant David Sheldon who can be contacted on (08) 8463 7700 or c/- Telecommunications Interception Section PO Box 1539, GPO Adelaide SA 5001.

Yours sincerely,

(Malcolm Hyde)
COMMISSIONER OF POLICE