Commonwealth OMBUDSMAN

Submission by the Commonwealth Ombudsman

INQUIRY INTO *TELECOMMUNICATIONS INTERCEPTION AND INTELLIGENCE SERVICES LEGISLATION AMENDMENT BILL 2010*

CONDUCTED BY THE SENATE STANDING COMMITTEE ON LEGAL AND CONSTITUTIONAL AFFAIRS

Submission by Mr Allan Asher

Commonwealth Ombudsman

October 2010

1 INTRODUCTION

On 30 September 2010, the Senate referred the *Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010* (the Bill) to the Senate Standing Committee on Legal and Constitutional Affairs (the Committee) for inquiry and report by 24 November 2010. The Committee has invited submissions on the Bill by 27 October 2010. I apologise for the delay in making the submission.

The Explanatory Memorandum states that the Bill will amend a number of Acts to enable greater co-operation, assistance and information sharing within Australia's law enforcement and national security communities. The Bill will specifically enable the Australian Security Intelligence Organisation (ASIO) to co-operate with and provide assistance to law enforcement agencies in relation to telecommunications interception and implements other measures in the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) that will improve access to stored communications.

2 BACKGROUND

The Commonwealth Ombudsman safeguards the community in its dealings with Australian Government agencies by:

- correcting administrative deficiencies through independent review of complaints about Australian Government action
- fostering good public administration that is accountable, lawful, fair, transparent and responsive
- reviewing statutory compliance by enforcement agencies in relation to:
    - telecommunications interceptions and access to stored communications under the TIA Act
    - use of surveillance devices under the *Surveillance Devices Act 2004*
    - conduct of controlled operations under Part 1AB of the *Crimes Act 1914*

The Commonwealth Ombudsman is responsible for reporting annually to the Attorney-General on enforcement agency (including the Australian Federal Police (AFP) and Australian Crime Commission (ACC)) compliance with the record keeping and destruction requirements relating to telecommunications interceptions. In addition, we report on the record keeping and destruction requirements relating to access to stored communications (e.g. email, SMS, etc) under the TIA Act and may report on other instances of non-compliance by officers of the law enforcement agencies.

The Ombudsman is also responsible for reporting to the Commonwealth Parliament biannually on law enforcement agency (including the AFP and ACC) activities under the *Surveillance Devices Act 2004* and annually under Part 1AB of the *Crimes Act 1914*.

The Ombudsman's oversight of the use of these covert powers by law enforcement agencies provides an important safeguard and assurance to the Commonwealth Parliament and the general community that these powers are properly exercised.

3 EXERCISE OF WARRANT POWERS

Under Chapter 2 of the TIA Act, the Ombudsman is required to inspect the records of the AFP, the ACC and the Australian Commission for Law Enforcement Integrity (ACLEI) twice a year. I do this to ascertain the extent of each agency's compliance with requirements to destroy restricted records, keep documents connected with the issue of warrants and keep records of interceptions. My office may also report any other contraventions of the TIA Act that come to our notice in the course of the inspection. I present reports on the results of inspections to the Attorney-General each year.

I note that the proposed amendments to s 55(3) of the TIA Act will include officers or employees of ASIO as those persons of another agency who may be approved to exercise the authority of a warrant. The proposal does not appear to introduce any fundamental changes in the exercise of warrant powers. However, as my office has no authority in respect of ASIO, interceptions undertaken by ASIO on behalf of other agencies may not be subject to the same level of scrutiny.

When inspecting the records of an agency, my officers interrogate the relevant interceptions system and, as one of a number of checks, ensure that no interceptions occurred outside the period the warrant was in force. Where ASIO executes a warrant on behalf of an agency that I would normally inspect, I will not be able to interrogate such systems. While oversight of ASIO is a responsibility of the Inspector-General of Intelligence and Security (IGIS), the TIA Act does not require IGIS to inspect the records of ASIO in these circumstances.

However, I note that the proposed amendments require ASIO to provide particulars of the interception to the agency that sought the warrant. My officers have discussed the practical implications of the proposed changes with the Attorney-General's Department and ASIO, and I understand that this would be provided by ASIO in the form of written records to the relevant agency. Those records would be available for my inspection. The logistics and record keeping proposed should assist in retaining an adequate, albeit different, oversight arrangement.

I also note that the level of compliance by the AFP and ACC with the requirements of the TIA Act in respect of telecommunication interceptions is generally high. The telecommunications interception regime has been in operation for a considerable period of time, and there is a good understanding by agencies of the legislative requirements and the process is automated with appropriate safeguards. I do not expect that to change with the proposed amendments.

4 WARRANTS RELATING TO VICTIMS

Under Chapter 3 of the TIA Act, the Ombudsman is required to inspect the records of enforcement agencies that relate to the access of stored communications, to ascertain the extent of compliance with the relevant provisions of the TIA Act. During 2009-10, I carried out 17 inspections of stored communications records maintained by 14 agencies.

Those agencies were the AFP, ACC, Australian Securities and Investments Commission, New South Wales Crime Commission, New South Wales Police, Queensland Police, Crime and Misconduct Commission (Queensland), South Australia Police, Tasmania Police, Victoria Police, Office of Police Integrity (Victoria), Western Australia Police, Corruption and Crime Commission (Western Australia) and Australian Customs and Border Protection Service.

Put simply, stored communications of a person involved in a serious contravention can be accessed with the knowledge of that person (or the sender of the stored communication) or under a warrant issued under the TIA Act.

The stored communications access scheme is designed to permit access to communications that have been stored by a carrier, rather than permitting enforcement agencies to monitor communications over a period of time, which would be akin to interception. This is particularly evident in the short period that a warrant remains in force, being five days from issue or until first executed.

In general, the level of controls and restrictions dictating who may access stored communications and for what purpose are set lower than the controls relating to telecommunications interception. This broader availability, together with the tighter timeframes, places a significant obligation on agencies to closely manage stored communications access if they are to be compliant with the TIA Act.

Schedule 4 of the Bill seeks to broaden the range of people in respect of whom a warrant can be sought, to include not only those persons who are being investigated for a serious contravention, but victims of that contravention. The Explanatory Memorandum states that this amendment clarifies whether s 116(1)(d) includes victims of a serious contravention.

I am of the view that the TIA Act does not presently allow a warrant to be sought in respect of a victim of a serious contravention. My inspections of agency records in 2009-10 have revealed a number of instances where the stored communications of victims were accessed. These instances of non-compliance were raised with the individual agencies concerned, and also reported to the Attorney-General in the Ombudsman's last two annual reports under the TIA Act. I am pleased to see that action has been taken by agencies to remedy this matter and that this issue has been recognised by the proposed amendments. That said, the amendment is but one of a number that are required in order to bring some clarity to a regime with significant compliance issues identified by my office.

These compliance issues were identified in the Ombudsman's report to the Attorney-General in 2008-09, although they were not included in the Attorney-General's report to Parliament under the TIA Act for the same period. I would be pleased to provide further information to the Committee on these issues.