Attachment A

Commonwealth OMBUDSMAN

Submission by the Commonwealth Ombudsman

INQUIRY INTO POTENTIAL REFORMS OF NATIONAL SECURITY LEGISLATION

Submission by the Acting Commonwealth Ombudsman, Alison Larkins

August 2012

1 Introduction

On 9 July 2012, the Parliamentary Joint Committee on Intelligence and Security (the Committee) commenced an inquiry into potential reforms of national security legislation (the inquiry). The Government has asked the Committee to consider a package of legislative reforms including to the telecommunications interception legislation, telecommunications sector security legislation and Australian intelligence community legislation. The inquiry will examine a number of key issues including safeguards and privacy protections, and clarity regarding the roles of the Commonwealth Ombudsman (the Ombudsman) and equivalent State bodies in overseeing telecommunications interception by law enforcement agencies.

This submission will focus on this latter aspect of the inquiry, taking into consideration the terms of reference and the accompanying discussion paper *Equipping Australia against emerging and evolving threats* (the discussion paper). This submission is informed by the Ombudsman's experience and insight gained from our inspection functions under the *Telecommunications (Interception and Access) Act 1979* (TIA Act) regarding law enforcement agencies' use of telecommunications interception and access to stored communications powers.

Overall, we welcome the proposed reforms to the TIA Act. Advancements in technologies, proliferation of communication methods and the increased importance to agencies of lawful interception of, and access to, communications reflect the need for a contemporary communications interception and access regime. Such a regime should be explicit and clear in its meaning, intention and safeguards, and provide for effective oversight of agencies' use of covert and intrusive powers.

This submission discusses:

- the oversight role of the Commonwealth Ombudsman, in particular, the need for greater clarity about our role and the desirability of a public reporting mechanism to improve transparency and accountability
- the importance of legislative safeguards and minimum standards to ensure agencies can sufficiently demonstrate compliance with the legislation
- the need for clarity in the TIA Act or any reformed legislation to ensure that it is practical for law enforcement agencies to comply.

2 Strengthening the safeguards and privacy protections under the lawful access to communications regime in the *Telecommunications (Interception and Access) Act 1979*

Oversight arrangements of the Commonwealth Ombudsman and State inspecting authorities

Publicly reporting on inspection activities

The purpose of an independent oversight mechanism, such as the Ombudsman and other inspecting authorities under the TIA Act, is to increase accountability and transparency and to maintain public confidence in agencies' use of covert and intrusive powers. Publicly reporting on whether agencies have used these powers lawfully is a key element in providing this accountability and transparency. However, the current provisions in the TIA Act do not

permit the Ombudsman to publicly report on our inspection activities and compliance assessments of agencies.

The current requirement is that the Ombudsman reports to the Commonwealth Attorney-General on the findings from inspections of telecommunications interception and stored communications access records. The Ombudsman's report is not made public. However, the Attorney-General is required to provide a summary of the Ombudsman's telecommunications interception inspection findings in their published annual report on the TIA Act. This requirement is not extended to our stored communications inspection findings and it is at the discretion of the Attorney-General as to what, if any, content is included in the Attorney-General's report.

In our view, this diminishes the effectiveness of the oversight mechanism. We have previously suggested to the Attorney-General's Department (AGD) that these provisions should be amended and a public reporting mechanism for the Ombudsman be introduced.

Currently, the Ombudsman publicly reports on our findings from inspections conducted under the *Surveillance Devices Act 2004* and Part IAB of the *Crimes Act 1914* – both acts confer convert and intrusive powers on law enforcement agencies. These published reports demonstrate our capacity to protect sensitive information while providing public accountability and transparency. The relevant provisions under these acts provide an appropriate model for a possible public reporting mechanism under the TIA Act.

Public reporting would also increase the Ombudsman's accountability and provide transparency of our methodologies and activities.

An example of an oversight body which publicly reports on telecommunications interception activities is the Interception of Communications Commissioner in the United Kingdom. The Commissioner publicly reports on their inspection activities, compliance assessments, and provides case studies of agencies' non-compliance.

Clarifying the role of the Ombudsman

Currently, the Ombudsman is only obliged to inspect agencies' compliance with the record keeping requirements of the TIA Act regarding the issue of warrants and the destruction of lawfully intercepted or accessed information. If a literal view of the current legislation were to be taken, the Ombudsman would only be required to determine if the agency has kept the records required under these provisions, rather than assess the veracity of these records. However, as we have access to those records required to be kept by agencies, we currently assess if agencies have met other requirements of the TIA Act, such as whether or not the warrants were obtained for a person who was actually involved in the relevant offence. This provides more robust oversight and assurance to the Attorney-General.

In our view, to remove any doubt about the Ombudsman's role and the purpose of our oversight, the Act could provide for a broader scope for the Ombudsman's oversight function. That is, it should include a clear requirement for the Ombudsman to ascertain agencies' compliance with the requirements of the Act (and not just whether or not certain

records were kept). This would align with the Ombudsman's inspection roles under the *Surveillance Devices Act 2004* and Part IAB of the *Crimes Act 1914*.

We have already raised this issue with the AGD in relation to the current legislation and note that page 26 of the discussion paper remarks that the current provisions of the TIA Act 'impede the Ombudsman's ability to report on possible contraventions and compliance issues.... rather than providing the Ombudsman scope to determine better ways of assisting agencies to meet their requirements'.

Currently, in addition to making a compliance assessment, we also suggest 'best practices' to agencies. Best practice issues often relate more to the intent of legislation and its proper use than record keeping requirements that receive 'compliance' assessments. The proposed approach to clarifying the Ombudsman's role would formalise our important role of commenting on best practice and encourage agencies to consider our suggestions.

An example of our best practice approach has been highlighting the importance of, and encouraging agencies to have in place, procedures that ensure that agencies are only dealing with lawfully accessed stored communications. These procedures involve monitoring all stored communications received by carriers to check that the accessed stored communications are those permitted by the warrant, and quarantining (i.e. not using for investigation purposes) any stored communications if there is any doubt about their lawfulness or insufficient information to determine their lawfulness.

Split oversight arrangements between the Commonwealth Ombudsman and State inspecting authorities

As noted in the discussion paper, there is currently a split between the oversight arrangements under the TIA Act, where the Ombudsman inspects the records of all Commonwealth, state and territory agencies[1] in respect of the stored communications access regime, compared to the telecommunications interception regime, where the Ombudsman only inspects Commonwealth agencies. [2]

As a result of inspecting all agencies' stored communication access records, we have been able to analyse if any identified issues are isolated or systemic in nature. For example, we have brought to the attention of the AGD a systemic issue relating to some agencies that were unable to determine if a carrier or service provider lawfully executed a stored communications warrant on their behalf.

As the period a stored communications warrant remains in force is limited, it is necessary for agencies to know the date it was executed by the carrier so agencies can assure themselves that they are dealing with lawfully obtained information. However, as identified during

[1] The agencies are: Australian Federal Police, Australian Crime Commission, Australian Customs and Border Protection Service, Australian Competition and Consumer Commission, Australian Securities and Investments Commission, the police forces of each state and the Northern Territory, Corruption and Crime Commission (WA), Crime and Misconduct Commission (QLD), Office of Police Integrity (VIC), New South Wales Crime Commission, and Police Integrity Commission (NSW).
[2] The Commonwealth agencies are: Australian Federal Police, Australian Crime Commission and Australian Commission for Law Enforcement Integrity.

numerous previous inspections, agencies were experiencing difficulty in obtaining this date. We have worked with the AGD to address this issue, and during more recent inspections, we noticed an improvement in agencies being able to obtain information concerning carriers' actions.

Options for further scrutiny of policing powers

In addition to the oversight functions provided for in the TIA Act, we note that there are other options available for the scrutiny of policing powers. For example, the New South Wales Ombudsman is required by NSW Parliament to review any new powers conferred on the NSW Police and provide a report regarding its findings to NSW Parliament.

The Committee may wish to consider this type of review function for the Ombudsman, particularly if any reformed legislation were to introduce new or significantly altered powers to intercept or access communications.

Mandatory record-keeping standards

The discussion paper notes on page 26, that 'consideration should be given to introducing new reporting requirements that are less process oriented and more attuned to providing the information needed to evaluate whether intrusion to privacy under the regime is proportionate to public outcomes'.

We do not have any objections to this approach but note that agency records are the best source of evidence to demonstrate compliance. The proposed flexible approach may be appropriate in accommodating current and future practices; however, we would expect that any reformed legislation would also include minimum record keeping standards.

The legislation's privacy protection objective

We note the proposal to include a privacy protection objective clause. If such an objective were introduced, in conducting oversight activities, we would expect that agencies would be able to demonstrate how they had met this objective when using their intrusive powers.

Currently, the emphasis is on the issuing authority (a Judge or nominated Administrative Appeals Tribunal member) to have regard to how much the privacy of any person or persons would be likely to be interfered with by intercepting or accessing communications authorised by the warrant.

Assessing to what extent an agency has met such an objective could form a part of the Ombudsman's inspection process, and this assessment could then be included in a published report.

3 Reforming the lawful access to communications regime

The standardisation of warrant tests and thresholds and expanding the basis of interception activities

We note the suggestion to standardise thresholds for all communications interception and access warrants. If this were to result in the lowering of the current thresholds, it is likely that there would be an increase in the number of warrants sought by agencies. There may also be an increase in the number of warrants, or other authorisation processes, if the basis of interception activities were expanded. Therefore, the Ombudsman's oversight and inspections work may increase as a consequence of these proposals. Consideration may need to be given to whether current resourcing of the office would enable an effective oversight regime.

Furthermore, if the basis of interception activities were expanded, we think it is preferable for there to be consistency in terms of warrant or authorisation procedures, safeguards and record keeping requirements. We would also expect that the proposed privacy protection objective would universally apply to all communications interception and access activities.

Reducing the number of agencies eligible to access communications information

Since the introduction of the stored communications regime in 2006, this office has inspected the records of 17 different enforcement agencies in relation to stored communications access to ensure compliance with the TIA Act. Some of these agencies include non-traditional law enforcement agencies, such as the Australian Competition and Consumer Commission, and the Australian Securities and Investments Commission. Other agencies eligible to apply the provisions include the Australian Tax Office and Centrelink.

We do not have a position on this proposal. Our only concern is that there is currently no obligation on agencies who have applied for a stored communications access warrant (or telecommunications interception warrant) to inform our office directly, so that we can conduct an inspection of their records and meet our statutory obligations under the TIA Act. Currently, near the end of each financial year, we have to contact every agency that is eligible to use the stored communications provisions, to ascertain warrant numbers and to plan for all inspections for the upcoming financial year.

We note that there is a current requirement under the TIA Act for agencies to report to the AGD as soon as practicable after the end of the financial year (after 30 June) on the number of warrants that were issued to each agency for the previous financial year. However, in order to meet our statutory requirements, we begin our inspections at the start of each financial year (from 1 July). It is therefore impracticable for us to wait until the AGD publishes these figures, which may not occur up until three months after we have begun our inspections.

We have previously recommended to the AGD that the TIA Act should include a provision that requires agencies that apply for a warrant under the TIA Act, or any reformed legislation,

to accordingly inform the Ombudsman or the relevant inspecting authority. This is to ensure oversight of all relevant agencies and that inspections occur in a timely manner.

4 Streamlining and reducing complexity in the lawful access to communications regime

Based on our inspection activities, we have identified a number of ambiguous provisions in the TIA Act, which may not be apparent even if intercepted or accessed communications are adduced as evidence in court. This creates uncertainty for agencies that have applied the relevant provisions with the intention of meeting their statutory obligations, invested resources in the related activities and relied on the intercepted or accessed communications. For example, under the TIA Act, a clear definition of 'execute' for a stored communications warrant is not provided. Consequently, at times we find it difficult to make definitive compliance assessments because of such ambiguities.

We note that some of these issues are a result of provisions which may not reflect current technologies or business practices. In our view, the proposed reforms to the TIA Act provide an opportunity to improve the clarity of provisions and introduce a contemporary regime that supports agencies in their law enforcement activities, while enabling them to comply and providing for effective oversight.

Creating a single warrant with multiple telecommunication interception powers and simplifying information sharing provisions

We note that the Government is considering simplifying the current warrant regime, which currently provides for four different types of warrants. We do not have any objections to this proposal; however we note that telecommunications and stored communications warrants are currently executed differently, and for stored communications warrants, possibly by more than one carrier. Therefore, these differences will need to be taken into consideration.

Whatever forms of warrant or warrants are proposed the relevant provisions need to be clear and explicit in their meaning and intent. For example, the definition of 'execute' of this proposed combined warrant will need to account for the different types of communications that may be intercepted and/or accessed, and take into account agency and industry business practices.

Additionally, we note the proposal to simplify the current information sharing arrangements of lawfully intercepted information to support cooperation between agencies. If this were to occur, we would anticipate safeguards to ensure agencies use and communicate lawfully intercepted information in accordance with the proposed privacy protection objective and other relevant provisions, and that agencies would be able to demonstrate this for inspection purposes.

5 Modernising the TIA Act's cost sharing framework

We note that consideration is being given to clarifying the Australian Communications and Media Authority's regulatory and enforcement role. As a general observation, agencies

currently rely on industry to lawfully execute stored communications warrants and to intercept communications on their behalf. However, if an employee of a carrier, for example, accesses stored communications in contravention of the TIA Act when providing a service to an agency, then that employee may be guilty of an offence. Furthermore, the evidentiary value of stored communications obtained by agencies may also be compromised if they are not lawfully accessed by that carrier.

Educating industry participants about their obligations and relevant provisions and prohibitions will empower industry to not only comply with the legislation but also support agencies in their important activities. We consider ongoing education to be fundamental for a successful regime, particularly given the increasing number of new entrants into the telecommunications industry.