NSW Ombudsman response to Attorney General's Department discussion paper "Equipping Australia against Emerging and Evolving Threats": Submission to the Parliamentary Joint Committee on Intelligence and Security, August 2012

Background

The Parliamentary Joint Committee on Intelligence and Security ("PJCIS") is inquiring into potential reforms of national security legislation. This submission relates specifically to the PJCIS inquiry into the *Telecommunications (Interception and Access) Act 1979* ("TIA Act") and makes references to the issues raised in relation to the TIA in the Attorney General's discussion paper "Equipping Australia against Emerging and Evolving Threats".

The NSW Ombudsman's interest in the PJCIS review of the TIA Act arises because of our role under the corresponding *Telecommunications (Interception and Access) (New South Wales) Act 1987* to undertake compliance inspections and monitoring of each of the agencies authorised to conduct interceptions in this state. As the NSW Act is complementary legislation, the issues we identify in the Commonwealth legislation are evident to us from our work in this area. The outcome of this review will consequently have a similar effect in NSW.

General comments

We note in the Introduction to the Discussion Paper the primary objective of the current TIA legislation is to protect the privacy of the users of telecommunications services in Australia. If agencies, bodies and individuals are to be permitted to breach privacy and deal with personal information as they see fit, there is no benefit to the community in having this legislation.

Our oversight and compliance monitoring role under the telecommunications interception legislation means our perspective is about ensuring the significant level of personal information gathered by law enforcement agencies under intercept is managed, used and stored in accordance with the applicable legislation and community expectations about privacy.

It is our view the TIA Act should be fully reviewed and rewritten to have regard to technological change and usage, and to incorporate current community expectations around privacy. Amendments to date have partially accommodated such changes but have generally resulted in the Act becoming increasingly difficult to properly interpret and implement. Related State legislation has consequently needed to 'keep up' and at times has lagged. At both levels this impacts on the inspection and oversight role this office holds.

Re-writing the TIA Act presents significant opportunities to government, including:

- A more up-to-date expression of the overarching need for the protection of people's privacy
- Clarification of the key objectives of the legislation
- Clarification for operational users about process and recording keeping, including access to, sharing of, use and retention of relevant information and records
- The removal of areas of duplication in process and record keeping
- Improving the type and form of record keeping required by agencies to demonstrate to inspectors their compliance with the legislation

- Reviewing the thresholds for matters in which interception may be used
- Reviewing how lawfully intercepted information may be used by authorities
- Satisfying any consequent need for additional methods or types of compliance and oversight.

We appreciate the fact that telecommunication interception has progressed well beyond the ambit of the original legislation and that the authorised law enforcement agencies must be in a position where they can keep up with technological change and the capacities available to offenders. However, it is our view any submissions for significant extension of powers under the TIA Act must be carefully considered from both an accountability and privacy perspective. The current requirements which ensure that intrusions are only permitted under carefully controlled circumstances are important elements of the Act, and careful consideration must be given to any proposal to weaken or reduce requirements serving accountability and control purposes.

If consideration is given to expanding or extending the provisions of the Act, these must be accompanied by a similar expansion or extension of the compliance and inspections requirements to ensure that the accountability and control frameworks continue to be effective and robust.

Comments specific to issues raised in the Discussion Paper

Strengthening the safeguards and privacy protections in line with contemporary community expectations

We support the inclusion in a reviewed TIA Act of the introduction of a specific privacy focused objects clause, as outlined on page 23 of the discussion paper.

Much of the need to review the legislation has arisen from the enormous change in the way people communicate and while expectations around the privacy of telephone conversations are understood, there is far less clarity – and greater concern – by many people about their other digital/electronic communications largely because of the interconnected nature of such communications and the wide range of media they incorporate. The Act needs to generally address privacy at all levels and to determine what may and may not be intercepted, for what purpose, and how it may be used.

A rewritten TIA Act should incorporate all oversight and access provisions for inspection and compliance purposes in one section to improve understanding and effectiveness. There should be an assurance that access powers relate to inspections but this should not be prescriptive, as this may work against any other proposals designed to improve the oversight regime.

For example, the possibility that access to content of communications by inspectors should be excluded has previously been flagged in discussions with the Commonwealth Attorney General's Department. Generally we agree inspection bodies do not need access to live communications as they occur but access to 'other' content of communications (for example 6(b) reports and affidavits among others) is necessary to ensuring compliance.

Reforming the lawful access regime

Through our compliance inspections under the NSW Act, we are aware both the Commonwealth, and consequently State, legislation contains areas of administrative inefficiency. Examples discussed with law enforcement agencies in the course of our inspections include the inability to delegate certain functions from chief officer or other similarly high ranking officer level, such as the role of

certifying officer, and the approval of destructions. The current requirements for high level staff to undertake these roles does not necessarily enhance accountability as those officers make decisions based on information provided by lower ranking staff in any event. Accountability may in fact be improved by making those who now recommend certain actions to Commissioners and Assistant Commissioners (for example) responsible instead for determining those matters, and certifying such decisions.

We are also aware from discussions with the agencies we inspect there is a desire for them to make greater use of 'by-product' interception material including for intelligence based activities. We do not generally support the Act being amended to include a free-range approach to the use of intercepted material extending to the general gathering of intelligence as this would be at odds with the intent of the legislation.

It is also our view that the ability to intercept should remain limited to those circumstances relating to the commission of certain serious offences, albeit with some further examination of the adequacy of the types of offences and the length of possible sentence currently authorised now being examined as part of the overall review of the Act.

Apart from our role of inspecting for compliance in relation to the interception of telecommunications, a question which has been raised by the NSW Police Force is whether the oversight and monitoring functions of the police complaints system in NSW by the NSW Ombudsman is a 'purpose connected with...an investigation of, or any inquiry into, alleged misbehaviour, or alleged improper conduct...".

The NSWPF and this office jointly sought advice from the NSW Solicitor General who opined that provision of telecommunications interception material to the NSW Ombudsman in performing its oversight and monitoring functions is a 'permitted purpose' under the TIA Act. This inquiry provides the opportunity to include in the legislation an appropriate authority for such use being a permitted purpose and to put the issue beyond doubt. Accordingly we suggest this as a provision to be included in the reviewed TIA Act.

<u>Streamlining and reducing complexity in the law</u>:

We submit it would be appropriate for the reviewed TIA Act to enable each State Ombudsman to inspect records relating to stored communications as well as Part 5-2 warrants. This would eliminate double handling of records, duplication of inspections and any related duality of compliance requirements. Such an inclusion would have the support of the agencies currently inspected in NSW, and no doubt other states.

At page 26 of the discussion paper options are canvassed with a view to changing the oversight inspection regime from one which is a process of administrative compliance checking to one where the inspector instead determines whether there is sufficient information held by the agency to demonstrate the use of these intrusive powers is proportional to the outcomes sought. There is clear benefit in the development of such a compliance regime. It is important the Act provides general prescription of the types of records maintained by each agency and at a minimum should require agencies to keep records which allow them to demonstrate that communications were:

- Obtained within the parameters of a warrant
- Used lawfully within the agency
- Communicated lawfully outside the agency

- Used in evidence lawfully
- Stored appropriately
- Destroyed lawfully

There is also room for the legislation to include the ability for the Commonwealth Ombudsman/State Ombudsman to either separately or jointly inquire into the use of an agency's powers under the Act, particularly if there is concern about compliance. Currently the prescribed record keeping method of compliance inspection does not envisage such inquiry. Including this activity would enhance accountability, and particularly in areas of interception where straight forward records may not be easily presented for inspection.

The Act should not prescribe a maximum number of inspections that an inspecting body may conduct in relation to any agency in any reporting period.

It is unclear why current legislation does not allow for public reporting on the outcomes of our inspections of agencies' use of telecommunications interception powers and their levels of compliance. We report to Parliament, and thereby to the community, on our similar activities under legislation covering both surveillance devices and controlled operations and would support the inclusion in the TIA Act of similar provisions for public reporting by all inspection bodies.

We also support the inclusion of provision within the legislation to enable inspection bodies to share areas of best practices, which may be identified during compliance inspections, across all agencies inspected.

Summary

We welcome the review of the *Telecommunications (Interception and Access) Act 1979* and the opportunity it presents to ensure both the legislation and the activities it permits are consistent with modern approaches to law enforcement and oversight, as well as the community's expectations their personal information and privacy will not be inappropriately intruded upon.

Bruce Barbour
NSW Ombudsman

20 August 2012