Ombudsman
New South Wales

NSW Ombudsman submission to The Senate Legal and Constitutional Affairs References Committee Inquiry into comprehensive revision of the *Telecommunications (Interception and Access) Act 1979*

Background

The Legal and Constitutional Affairs References Committee has received a reference from The Senate to inquire into, and report on, the:

> "Comprehensive revision of the *Telecommunications (Interception and Access) Act 1979* (the Act), with regard to:
>
> (a) the recommendations of the Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* report, dated May 2008, particularly recommendation 71.2; and
>
> (b) recommendations relating to the Act from the Parliamentary Joint Committee on Intelligence and Security *Inquiry into the potential reforms of Australia's National Security Legislation* report, dated May 2013.

The NSW Ombudsman has been invited to make a submission addressing the terms of reference. Our interest in the 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.

In August 2012, we made a submission to the Parliamentary Joint Committee on Intelligence and Security ("PJCIS") Inquiry referred to above, and also participated in the collective submission made by the NSW Government to that inquiry. Much of what is contained in this document reiterates our comments made to the previous inquiry.

General observations

The generally accepted objective of the current Act is the protection of 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. The current Act, however, does not contain any specific "Objects" as is included in other more recent legislation, such as the *Telecommunications Act 1997*. The inclusion of an "Objects" section in the Act is considered an important starting point for redrafting the 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.

Ombudsman
New South Wales

In general, our overarching view is consistent with Recommendation 18 of the PJCIS report, that the Act be comprehensively revised to design an interception regime which is underpinned by the protection of privacy, is technologically neutral, maintains investigative capabilities for lawful purposes, articulates enforceable obligations and supports robust oversight and accountability, and administrative efficiency.

We note the PJCIS also recommended further consultation with stakeholders and for a revised Act to be released as an exposure draft with the views of key agencies, including ombudsmen and the Inspector General of Intelligence and Security, being sought. In a legislative arrangement such as this, where national consistency is crucial to the efficient and effective operation of the scheme, and as whatever is legislated by the Commonwealth must then be reflected in complementary state and territory Acts, an exposure draft is an essential step in helping to identify any unintended consequences or practical problems or flaws associated with any proposed changes. Nevertheless, this submission is made without the benefit of such an exposure draft of a reviewed Act and so our comments remain of a general nature.

Once again we note, re-drafting the Act presents significant opportunities to government, including:

- A more up-to-date expression of the need for the protection of people's privacy
- Clarification of the key objectives of the legislation
- Clarification for operational users about process and record 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 compliance with the legislation to inspectors
- Addressing concerns about thresholds for matters in which interceptions may be used
- Reviewing the use by authorities of lawfully intercepted information
- Satisfying any consequent need for additional methods or types of compliance and oversight.

Comments specific to recommendations contained in the PJCIS report of May 2013

Our focus in these comments is on those recommendations directly related to our role in relation to compliance and oversight. To this end we offer general support for all recommendations focussed on ensuring the privacy of individuals is maintained.

Recommendation 4

> *The Committee recommends that the Attorney-General's Department undertake a review of the oversight arrangements to consider the appropriate organisation or agency to ensure effective accountability under the Telecommunications (Interception and Access) Act 1979.*
>
> *Further, the review should consider the scope of the role to be undertaken by the relevant oversight mechanism.*

Ombudsman
New South Wales

The Committee also recommends the Attorney General's Department consult with State and Territory ministers prior to progressing any proposed reforms to ensure jurisdictional considerations are addressed.

We agree with this recommendation which addresses the need for oversight arrangements to be an essential part of a review of the Act.

Later recommendations refer to the roles of various Ombudsman offices in the oversight and compliance regime for the Act. How the oversight and compliance regime will operate, and what it will include will of course ultimately depend on what is included in the redrafted Act. It is anticipated, nevertheless, based on the later recommendations in the PJCIS report, that any redrafted Act would encompass a more broad-based approach to compliance and oversight than simple record keeping checks, and we would support such an approach.

Recommendation 7

The Committee recommends that interception be conducted on the basis of specific attributes of communications.

The Committee further recommends that the Government model 'attribute based interception' on the existing named person interception warrants, which includes:

- *the ability for the issuing authority to set parameters around the variation of attributes for interception;*
- *the ability for interception agencies to vary the attributes for interception; and*
- *reporting on the attributes added for interception by an authorised officer within an interception agency.*

In addition to Parliamentary oversight, the Committee recommends that attribute based interception be subject to the following safeguards and accountability measures:

- *attribute based interception is only authorised when an issuing authority or approved officer is satisfied the facts and grounds indicate that interception is proportionate to the offence or national security threat being investigated;*
- *oversight of attribute based interception by the ombudsmen and Inspector-General of Intelligence and Security; and*
- *reporting by the law enforcement and security agencies to their respective Ministers on the effectiveness of attribute based interception.*

The recommendation relates to a redrafted Act enabling interception to be conducted on the basis of specific attributes of communications. The recommendation suggests such interception is modelled on the current named person interception warrant and should include parameters to be set by the issuing authority, for interception agencies to be able to vary the attributes for interception, and for an authorised officer in an interception agency to report on attributes added for interception.

This significantly enhances the interception capabilities of the agency and consequently the recommendation goes on to make reference to the need for additional safeguards and accountability measures over and above Parliamentary oversight. The recommendation

suggests that attribute based interception should be authorised only when it is proportionate to the offence or the threat to national security disclosed in the facts and grounds presented, that there be oversight by Ombudsman and Inspector General of Intelligence and Security of attribute based interception, and for specific reports to be made to respective Ministers on the effectiveness of this form of interception.

We agree with the recommendation of the PJCIS that an attribute based form of interception should only be introduced along with the additional safeguards and accountabilities outlined above, being specifically included in any redrafted Act.

Recommendation 10

> *The Committee recommends that the telecommunications interception warrant provisions in the Telecommunications (Interception and Access) Act 1979 be revised to develop a single interception warrant regime.*
>
> *The Committee recommends the single warrant regime include the following features:*
>
> - *a single threshold for law enforcement agencies to access communications based on serious criminal offences;*
> - *removal of the concept of stored communications to provide uniform protection to the content of communications; and*
> - *maintenance of the existing ability to apply for telephone applications for warrants, emergency warrants and ability to enter premises*
>
> *The Committee further recommends that the single warrant regime be subject to the following safeguards and accountability measures:*
>
> - *interception is only authorised when an issuing authority is satisfied the facts and grounds indicate that interception is proportionate to the offence or national security threat being investigated;*
> - *rigorous oversight of interception by ombudsmen and Inspector-General of Intelligence and Security;*
> - *reporting by the law enforcement and security agencies to their respective Ministers on the effectiveness of interception; and*
> - *Parliamentary oversight of the use of interception.*

This recommendation refers to the adoption of a single warrant regime, along with the removal of the concept of stored communications, and the maintenance of the existing ability to make telephone applications for warrants, for emergency warrants and to enter premises.

We believe adopting this recommendation would be an important step toward achieving a consistent and more administratively efficient telecommunication interception warrant regime.

The further provisions of this Recommendation cover the authorisation of an interception by an issuing authority being a proportionate response to the offence or national security threat being investigated, rigorous oversight of interception, reporting by the user agencies to their respective Ministers about the effectiveness of interception, and Parliamentary oversight.

We agree with the view encapsulated in this Recommendation that the single warrant regime should be adopted and that such adoption must be accompanied by rigorous oversight provided by the various Ombudsman and the Inspector-General of Intelligence and Security. These oversight agencies are already well placed to do this, having extensive experience of maintaining independence and providing transparency within an environment where national security is protected and serious crimes are investigated, without hindering the privacy of individuals beyond the provisions of the legislation.

Recommendation 18

> *The Committee recommends that the Telecommunications (Interception and Access) Act 1979 (TIA Act) be comprehensively revised with the objective of designing an interception regime which is underpinned by the following:*
> - *clear protection for the privacy of communications;*
> - *provisions which are technology neutral;*
> - *maintenance of investigative capabilities, supported by provisions for appropriate use of intercepted information for lawful purposes;*
> - *clearly articulated and enforceable industry obligations; and*
> - *robust oversight and accountability which supports administrative efficiency.*
>
> *The Committee further recommends that the revision of the TIA Act be undertaken in consultation with interested stakeholders, including privacy advocates and practitioners, oversight bodies, telecommunications providers, law enforcement and security agencies.*
>
> *The Committee also recommends that a revised TIA Act should be released as an exposure draft for public consultation. In addition, the Government should expressly seek the views of key agencies, including the:*
> - *Independent National Security Legislation Monitor;*
> - *Australian Information Commissioner;*
> - *Ombudsmen and the Inspector-General of Intelligence and Security.*
>
> *In addition, the Committee recommends the Government ensure that the draft legislation be subject to Parliamentary committee scrutiny.*

The recommendation deals specifically with the need to comprehensively revise the Act to ensure its objects and the capabilities it provides are consistent with current expectations of the community and the needs of law enforcement and security agencies. All parties involved have agreed for several years such a revision is required. The Act as currently written is somewhat out of date, inconsistent and inefficient administratively. Currently oversight is also mechanistic and there is room for the review to address this to further enhance accountability.

It has been previously suggested the oversight inspection regime should move from one which is a process of administrative compliance checking to one where the inspector instead determine whether there is sufficient information held by the agency to demonstrate the use of these powers in 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 to be 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 redrafted 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 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 Act of similar provisions for public reporting by all inspection bodies.

Clarification of a specific 'permitted purpose'

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

The NSW Police Force 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. The potential redrafting of the legislation provides an opportunity to include in the Act 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 as outlined in (vi) below:

"permitted purpose", in relation to an interception agency, an eligible Commonwealth authority or an eligible authority of a State, means a purpose connected with:

...

(c) in the case of the Police Force of a State:

(i) an investigation of, or an inquiry into, alleged misbehaviour, or alleged improper conduct, of an officer of that State, being an investigation or inquiry under a law of that State or by a person in the person's capacity as an officer of that State; or

(ii) a report on such an investigation or inquiry; or

Ombudsman
New South Wales

(iia) the making by a person of a decision in relation to the appointment, re-appointment, term of appointment, retirement or termination of appointment of an officer or member of staff of that Police Force; or

(iib) a review (whether by way of appeal or otherwise) of such a decision; or

(iii) the tendering to the Governor of that State of advice to terminate, because of misbehaviour or improper conduct, the appointment of an officer of that State; or

(iv) deliberations of the Executive Council of that State in connection with advice to the Governor of that State to terminate, because of misbehaviour or improper conduct, the appointment of an officer of that State; or

(v) the performance of a function or duty, or the exercise of a power, by a person, court or other body under, or in relation to a matter arising under, an organised crime control law of that State;

(vi) the performance of a function or duty, or the exercise of a power, by the Commissioner of the NSW Police Force or the NSW Ombudsman under Part 8A of the Police Act or a cognate law of that State.

Section 5 of the TIA Act would need to include the following new definition:

"Police Act" means the *Police Act 1990* of New South Wales.

In addition, it is our view that consideration should be given to an amendment to expand the definition of 'permitted purpose' under sub section (iia) to include the types of decisions taken in response to police misconduct under section 173(2) of the *Police Act 1990* which include

- reduction of the police officer's rank or grade,
- a reduction of the police officer's seniority,
- a deferral of the police officer's salary increment

Summary

While providing the above comments on specific matters, we strongly support the recommendation of the PJCIS, set out in its report of May 2013, that the *Telecommunications (Interception and Access) Act 1979* be comprehensively reviewed, and that a revised Act should be released as an exposure draft for publication consultation. We also support the recommendation for the express views of key agencies including the Independent National Security Legislation Monitor, Australian Information Commissioner, Commonwealth and State Ombudsman and the Inspector- General of Intelligence and Security to be sought and would welcome the opportunity to provide such views on an exposure draft of the revised legislation.

Bruce Barbour
NSW Ombudsman

27 February 2014