Comments from Opposition Senators

The Opposition notes the earlier inquiries into the telecommunications interception regime in Australia, referred to in Chapter 1 of this report. In particular, the Opposition notes that following a year of extensive consultation and detailed consideration, in June 2013 the Parliamentary Joint Committee on Intelligence and Security (PJCIS) tabled a unanimous report recommending wide-ranging reforms to Australia's national security legislation. In particular, the PJCIS conducted a comprehensive review of the *Telecommunications (Interception and Access) Act 1979* (TIA Act), and in Chapter 2 of its 2013 Report made 18 recommendations for improvements to that legislative framework.

Labor members of this Committee endorse Recommendation 18 of the 2013 PJCIS Report, which states:

> 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.

Although the 2013 Report of the PJCIS was unanimous, and included the current Attorney-General as one of its members at the time, the Abbott Government has still not responded to the recommendations in Chapter 2, let alone commenced the considerable work outlined in Recommendation 18 above. Labor is also concerned that the Abbott Government chose to ignore the recommendations for a

comprehensive review of the TIA Act while pressing ahead with the introduction of a new data retention regime in the form of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Data Retention Bill). It is clear to Labor members of this Committee that improving the legislative framework for telecommunications interception and access should have been undertaken prior to the introduction of a mandatory data retention regime, which necessarily relies on the existing, and now outdated, TIA Act framework.

Labor Members of this Committee also note that in its February 2015 *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, the PJCIS recommended that 'the Government provide a response to the outstanding recommendations from the Committee's 2013 *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* by 1 July 2015'. Labor members of this Committee endorse this recommendation of the PJCIS, noting that eighteen of the nineteen outstanding recommendations referred to relate to reform of the TIA Act. We have reproduced below the 18 recommendations of the PJCIS from the June 2013 Report relating to the TIA Act, and call on the Government to formally accept all of these recommendations and to commence as soon as practicable the revision of that Act.

Labor members of this Committee also take this opportunity to express our disappointment at the chaotic and unnecessarily rushed manner in which the Abbott Government approached the Data Retention Bill. The Abbott Government did nothing to progress data retention laws during its first year in office, preferring to instead focus its energies on campaigns such as its failed attempt to repeal the race hate provisions in section 18C of the *Racial Discrimination Act 1975*. Despite failing to act on data retention laws for over a year in office, when it finally decided to act on data retention the Abbott Government claimed that the matter was suddenly of great urgency. The Government then chose to ignore the unanimous 2013 recommendation of the PJCIS to release an exposure draft of the proposed legislation for consultation, and instead introduced a significantly flawed bill into the Parliament. Now infamous attempts by senior members of the Government to explain the Bill in the weeks after its introduction only created confusion that exacerbated public concern about the effects of the proposed legislation.

The Government then sought to rush the review of the Data Retention Bill by the PJCIS, pressing for the Bill to be reviewed with an urgency that would have precluded proper public scrutiny. However, Labor insisted that the Government allow time for proper consideration of the Bill by the PJCIS, including adequate time for the public, legal bodies and key stakeholders to make submissions, and for public hearings to be held.

The review of the Data Retention Bill by the PJCIS revealed how flawed the Government's proposed legislation was. In its 2015 report the PJCIS made 38 substantive recommendations for changes to the Bill to improve the efficacy of the proposed regime, while at the same time introducing significant improvements to the data security, oversight and accountability mechanisms under which the proposed

regime would operate. Those recommendations were all accepted by the Government, and required numerous amendments to the Bill.

Labor members of this Committee strongly suggest that the Government take a more sensible, measured and consultative approach to reform of the TIA Act. Specifically, Labor recommends that the Government does not again ignore the bipartisan recommendations of the PJCIS, and follows the recommendation to revise the TIA Act in consultation with relevant stakeholders and to release an exposure draft of a revised TIA Act for public consultation and for consideration by the PJCIS.

Recommendations of the 2013 PJCIS Report with respect to telecommunications interception

Recommendation 1

The Committee recommends the inclusion of an objectives clause within the *Telecommunications (Interception and Access) Act 1979*, which:

- expresses the dual objectives of the legislation
- to protect the privacy of communications;
- to enable interception and access to communications in order to investigate serious crime and threats to national security; and
- accords with the privacy principles contained in the *Privacy Act 1988*.

Recommendation 2

The Committee recommends the Attorney-General's Department undertake an examination of the proportionality tests within the *Telecommunications (Interception and Access) Act 1979* (TIA Act). Factors to be considered in the proportionality tests include the:

- privacy impacts of proposed investigative activity;
- public interest served by the proposed investigative activity, including the gravity of the conduct being investigated; and
- availability and effectiveness of less privacy intrusive investigative techniques.

The Committee further recommends that the examination of the proportionality tests also consider the appropriateness of applying a consistent proportionality test across the interception, stored communications and access to telecommunications data powers in the TIA Act.

Recommendation 3

The Committee recommends that the Attorney-General's Department examine the *Telecommunications (Interception and Access) Act 1979* with a view to revising the reporting requirements to ensure that the information provided assists in the

evaluation of whether the privacy intrusion was proportionate to the public outcome sought.

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.

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.

Recommendation 5

The Committee recommends that the Attorney-General's Department review the threshold for access to telecommunications data. This review should focus on reducing the number of agencies able to access telecommunications data by using gravity of conduct which may be investigated utilising telecommunications data as the threshold on which access is allowed.

Recommendation 6

The Committee recommends that the Attorney-General's Department examine the standardisation of thresholds for accessing the content of communications. The standardisation should consider the:

- privacy impact of the threshold;
- proportionality of the investigative need and the privacy intrusion;
- gravity of the conduct to be investigated by these investigative means;
- scope of the offences included and excluded by a particular threshold; and
- impact on law enforcement agencies' investigative capabilities, including those accessing stored communications when investigating pecuniary penalty offences.

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.

Recommendation 8

The Committee recommends that the Attorney-General's Department review the information sharing provisions of the *Telecommunications (Interception and Access) Act 1979* to ensure:

- protection of the security and privacy of intercepted information; and
- sharing of information where necessary to facilitate investigation of serious crime or threats to national security.

Recommendation 9

The Committee recommends that the *Telecommunications (Interception and Access) Act 1979* be amended to remove legislative duplication.

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 the 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.

Recommendation 11

The Committee recommends that the Government review the application of the interception-related industry assistance obligations contained in the *Telecommunications (Interception and Access) Act 1979* and *Telecommunications Act 1997*.

Recommendation 12

The Committee recommends the Government consider expanding the regulatory enforcement options available to the Australian Communications and Media Authority to include a range of enforcement mechanisms in order to provide tools proportionate to the conduct being regulated.

Recommendation 13

The Committee recommends that the *Telecommunications (Interception and Access) Act 1979* be amended to include provisions which clearly express the scope of the obligations which require telecommunications providers to provide assistance to law enforcement and national security agencies regarding telecommunications interception and access to telecommunications data.

Recommendation 14

The Committee recommends that the *Telecommunications (Interception and Access Act) 1979* and the *Telecommunications Act 1997* be amended to make it clear beyond doubt that the existing obligations of the telecommunications interception regime apply to all providers (including ancillary service providers) of telecommunications services accessed within Australia. As with the existing cost sharing arrangements, this should be done on a no-profit and no-loss basis for ancillary service providers.

Recommendation 15

The Committee recommends that the Government should develop the implementation model on the basis of a uniformity of obligations while acknowledging that the creation of exemptions on the basis of practicability and affordability may be

justifiable in particular cases. However, in all such cases the burden should lie on the industry participants to demonstrate why they should receive these exemptions.

Recommendation 16

The Committee recommends that, should the Government decide to develop an offence for failure to assist in decrypting communications, the offence be developed in consultation with the telecommunications industry, the Department of Broadband Communications and the Digital Economy, and the Australian Communications and Media Authority. It is important that any such offence be expressed with sufficient specificity so that telecommunications providers are left with a clear understanding of their obligations.

Recommendation 17

The Committee recommends that, if the Government decides to develop timelines for telecommunications industry assistance for law enforcement and national security agencies, the timelines should be developed in consultation with the investigative agencies, the telecommunications industry, the Department of Broadband Communications and the Digital Economy, and the Australian Communications and Media Authority.

The Committee further recommends that, if the Government decides to develop mandatory timelines, the cost to the telecommunications industry must be considered.

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.

Conclusion

Labor will always work to keep our nation safe, and at the same time to uphold the rights and freedoms enjoyed by all Australians. Getting this balance right can be a challenging task, and it is clear that there is still work to do to ensure that Australia's national security and law enforcement legislation meets the needs of our agencies while at the same time incorporating robust and effective oversight mechanisms and safeguards.

For example, Labor will continue to press for improvements to data security through the Telecommunications Sector Security Reform (TSSR) process. The TSSR aims to identify, manage and mitigate national security risks associated with Australia's telecommunications infrastructure, including matters such as the physical location of stored telecommunications data. This was also the subject of the PJCIS's 2013 report, which included at Recommendation 19:

> The Committee recommends that the Government amend the *Telecommunications Act 1997* to create a telecommunications security framework that will provide:
>
> - a telecommunications industry-wide obligation to protect infrastructure and the information held on it or passing across it from unauthorised interference;
> - a requirement for industry to provide the Government with information to assist in the assessment of national security risks to telecommunications infrastructure; and
> - powers of direction and a penalty regime to encourage compliance.

These PJCIS also recommended that the TSSR be subject to a comprehensive regulatory impact assessment.

In addition to the TSSR process, Senator John Faulkner, who retired from the Parliament in February this year, advocated for further improvements to the transparency and accountability mechanisms in our national security frameworks. It was Senator Faulkner's view that it is the Parliament to which our police and national security agencies are ultimately accountable, and it is the Parliament's responsibility to oversee their priorities and effectiveness, and to ensure that our agencies meet the requirements and standards that Parliament sets.

To this end Senator Faulkner developed a set of reforms designed to ensure that the effectiveness of Parliamentary oversight of intelligence and security agencies keeps pace with any enhanced powers being given to those agencies. A key reform

recommended by Senator Faulkner was for the PJCIS to have oversight of certain operational matters of the security agencies. Progress towards that reform is evident in the Data Retention Bill, which Labor pressed to be amended so that the PJCIS could oversight aspects of the data retention scheme.

Labor will bring forward legislation this year to give effect to the wider reforms proposed by Senator Faulkner.

Labor believes that ensuring the ongoing efficacy and integrity of our national security architecture is an ongoing responsibility of all parliamentarians, and Labor will continue to engage constructively in this important process.

Senator Jacinta Collins
Labor Senator for Victoria