Appendix 1

Recommendations 1 to 18, 42 and 43 of the PJCIS Report of the Inquiry into Potential Reforms of Australia's National Security Legislation

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. xxvi

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.

Recommendation 42

- There is a diversity of views within the Committee as to whether there should be a mandatory data retention regime. This is ultimately a decision for Government. If the Government is persuaded that a mandatory data retention regime should proceed, the Committee recommends that the Government publish an exposure draft of any legislation and refer it to the Parliamentary Joint Committee on Intelligence and Security for examination. Any draft legislation should include the following features:
  - any mandatory data retention regime should apply only to meta-data and exclude content;
  - the controls on access to communications data remain the same as under the current regime;
  - internet browsing data should be explicitly excluded;
  - where information includes content that cannot be separated from data, the information should be treated as content and therefore a warrant would be required for lawful access;
  - the data should be stored securely by making encryption mandatory;
  - save for existing provisions enabling agencies to retain data for a longer period of time, data retained under a new regime should be for longer period of time, data retained under a new regime should be for no more than two years;
  - the costs incurred by providers should be reimbursed by the Government;
  - a robust, mandatory data breach notification scheme;
  - an independent audit function be established within an appropriate agency to ensure that communications content is not stored by telecommunications service providers; and
  - oversight of agencies' access to telecommunications data by the ombudsmen and the Inspector-General of Intelligence and Security.

Recommendation 43

- The Committee recommends that, if the Government is persuaded that a mandatory data retention regime should proceed:
  - there should be a mechanism for oversight of the scheme by the Parliamentary Joint Committee on Intelligence and Security;
  - there should be an annual report on the operation of this scheme presented to Parliament; and

- the effectiveness of the regime be reviewed by the Parliamentary Joint Committee on Intelligence and Security three years after its commencement.