B

Appendix B – Recommendations from PJCIS report of May 2013

Source: Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, Canberra, May 2013.

List of recommendations - 2013 report

2 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.

3 Telecommunications security

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.

The Committee further recommends that the Government, through a Regulation Impact Statement, address:

- the interaction of the proposed regime with existing legal obligations imposed upon corporations;
- the compatibility of the proposed regime with existing corporate governance where a provider's activities might be driven by decisions made outside of Australia;
- consideration of an indemnity to civil action for service providers who have acted in good faith under the requirements of the proposed framework; and
- impacts on competition in the market-place, including:
  - ⇒ the potential for proposed requirements to create a barrier to entry for lower cost providers;
  - ⇒ the possible elimination of existing lower cost providers from the market, resulting in decreased market competition on pricing; and
  - ⇒ any other relevant effects.

4 Australian Intelligence Community Legislation Reform

Recommendation 20

The Committee recommends that the definition of computer in the *Australian Security Intelligence Organisation Act 1979* be amended by adding to the existing definition the words "and includes multiple computers operating in a network".

The Committee further recommends that the warrant provisions of the ASIO Act be amended by stipulating that a warrant authorising access to a computer may extend to all computers at a nominated location and all computers directly associated with a nominated person in relation to a security matter of interest.

Recommendation 21

The Committee recommends that the Government give further consideration to amending the warrant provisions in the *Australian Security Intelligence Organisation Act 1979* to enable the disruption of a target computer for the purposes of executing a computer access warrant but only to the extent of a demonstrated necessity. The Committee

further recommends that the Government pay particular regard to the concerns raised by the Inspector-General of Intelligence and Security.

Recommendation 22

The Committee recommends that the Government amend the warrant provisions of the *Australian Security Intelligence Organisation Act 1979* to allow ASIO to access third party computers and communications in transit to access a target computer under a computer access warrant, subject to appropriate safeguards and accountability mechanisms, and consistent with existing provisions under the *Telecommunications (Interception and Access) Act 1979*.

Recommendation 23

The Committee recommends the Government amend the warrant provisions of the *Australian Security Intelligence Organisation Act 1979* to promote consistency by allowing the Attorney-General to vary all types of ASIO Act warrants.

Recommendation 24

Subject to the recommendation on renewal of warrants, the Committee recommends that the maximum duration of *Australian Security Intelligence Organisation Act 1979* search warrants not be increased.

Recommendation 25

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to allow the Attorney-General to renew warrants.

Recommendation 26

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to modernise the Act's provisions regarding secondment arrangements.

Recommendation 27

The Committee recommends that the *Intelligence Services Act 2001* be amended to clarify the authority of the Defence Imagery and Geospatial Organisation to undertake its geospatial and imagery functions.

Recommendation 28

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to create an authorised intelligence operations scheme, subject to similar safeguards and accountability arrangements as apply to the Australian Federal Police controlled operations regime under the *Crimes Act 1914*.

Recommendation 29

The Committee recommends that should the Government proceed with amending the *Australian Security Intelligence Organisation Act 1979* to establish a named person warrant, further consideration be given to the factors that would enable ASIO to request a single warrant specifying multiple powers against a single target. The thresholds, duration, accountability mechanisms and oversight arrangements for such warrants should not be lower than other existing ASIO warrants.

Recommendation 30

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to modernise the warrant provisions to align the surveillance device provisions with the *Surveillance Devices Act 2004,* in particular by optical devices.

Recommendation 31

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* not be amended to enable person searches to be undertaken independently of a premises search.

Recommendation 32

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to establish classes of persons able to execute warrants.

Recommendation 33

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to formalise ASIO's capacity to co-operate with private sector entities.

Recommendation 34

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended so that ASIO may refer breaches of section 92 to law enforcement for investigation.

Recommendation 35

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to clarify that the incidental power in the search and computer access warrant provisions includes entry to a third party's premises for the purposes of executing those warrants. However, the Committee is of the view that whatever amendments are made to facilitate this power should acknowledge the exceptional nature and very limited circumstances in which the power should be exercised.

Recommendation 36

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to clarify that reasonable force can be used at any time for the purposes of executing the warrant, not just on entry, and may only be used against property and not persons.

Recommendation 37

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to introduce an evidentiary certificate regime to protect the identity of officers and sources. The Committee also recommends that similar protections be extended to ASIO in order to protect from disclosure in open court its sensitive operational capabilities, analogous to the provisions of the *Telecommunications (Interception and Access) Act 1979* and the protections contained in the counter terrorism provisions in the Commonwealth Criminal code.

The Committee further recommends that the Attorney-General give consideration to making uniform across Commonwealth legislation provisions for the protection of certain sensitive operational capabilities from disclosure in open court.

Recommendation 38

The Committee recommends that the *Intelligence Services Act 2001* be amended to add a new ministerial authorisation ground where the Minister is satisfied that a person is, or is likely to be, involved in intelligence or counter-intelligence activities in circumstances where such an investigation would not currently be within the operational authority of the agency concerned.

Recommendation 39

The Committee recommends that where ASIO and an *Intelligence Services Act 2001* agency are engaged in a cooperative intelligence operation a common standard based on the standards prescribed in the *Australian Security Intelligence Organisation Act 1979* should apply for the authorisation of intrusive activities involving the collection of intelligence on an Australian person.

Recommendation 40

The Committee recommends that the *Intelligence Services Act 2001* be amended to enable ASIS to provide training in self-defence and the use of weapons to a person cooperating with ASIS.

Recommendation 41

The Committee recommends that the draft amendments to the *Australian Security Intelligence Organisation Act 1979* and the *Intelligence Services Act 2001*, necessary to give effect to the Committee's recommendations, should be released as an exposure draft for public consultation. The Government should expressly seek the views of key stakeholders, including the Independent National Security Legislation Monitor and Inspector-General of Intelligence and Security.

In addition, the Committee recommends the Government ensure that the draft legislation be subject to Parliamentary committee scrutiny.

5 Data Retention

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 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.