Submission No 114

Inquiry into potential reforms of National Security Legislation

Organisations: Australian Mobile Telecommunications Association and Communications Alliance

"EQUIPPING AUSTRALIA AGAINST EMERGING AND EVOLVING THREATS"

An Inquiry into Potential Reforms of National Security Legislation

Submission on the Terms of Reference
and Discussion Paper as prepared by:

Australian Mobile Telecommunications Association and Communications Alliance

and endorsed by:

Australian Information Industry Association and Australian Industry Group

20 August 2012

Executive Summary

The Australian Mobile Telecommunications Association and Communications Alliance (the Associations) welcome the opportunity to comment on the package of potential reforms to existing national security legislation under inquiry by the Parliamentary Joint Committee on Intelligence and Security (PJCIS). The Attorney-General's Department (AGD) has proposed fundamental changes to regulatory obligations that will necessarily have a significant impact on the telecommunications industry. The form of this impact is outlined in later sections of this response.

Of note is the formal endorsement of the positions represented by the Associations in this submission by both the Australian Information Industry Association (AIIA)[1], and the Australian Industry Group (Ai Group)[2].

These endorsements highlight the very broad cross-sectoral support for the views being advanced by the Associations and point to the fact that the proposed reforms have significant implications not just for the Australian ICT sector, but for all businesses and individuals using telecommunications products and services in this country.

The Associations support the objectives underlying the reform package – i.e. the need to ensure that Australia's network infrastructure is secure against external threats and that agencies can move swiftly and effectively to secure the information reasonably required to detect criminal activity or counter threats from individuals or organisations.

While the terms of reference for this Inquiry refer to "the fact that national security brings shared responsibilities to the government and the private sector", many of the proposed reforms are likely to shift onto industry numerous responsibilities, costs, and risks that have traditionally rested with Government and its agencies.

While recognising the proposals reflect the difficulty of achieving some security-related objectives in an increasingly complex market environment, the Associations strongly believe that industry should not be asked to assume risks and responsibilities that properly rest with Government.

The full and real economic cost of providing assistance to national security and enforcement agencies must be minimised (to avoid costs being passed onto consumers) and be recoverable from agencies that will benefit from access to such information.

Similarly, any costs associated with a requirement to retain customers' communications data not normally retained for business purposes, should not be borne by industry.

Lawful interception must continue to be subject to appropriate checks and balances. The onus should remain with intercepting agencies to clearly identify the person of interest and all target services on an interception warrant. Industry should not bear any responsibility for having to interpret a warrant or identify services that should or should not be intercepted when a warrant is served. Decisions about such matters should occur prior to any independent oversight, not afterwards. The requirements for industry interception obligations

[1] http://www.aiia.com.au/

[2] http://www.aigroup.com.au/

should also be clear, straightforward, proportionate and reasonable without being overly prescriptive or onerous. While obligations and outcomes need to be clearly defined, regulatory and legislative requirements should not be so prescriptive or detailed that they define how those obligations and outcomes should be met. Industry must have flexibility in delivering the required outcomes in the most efficient and economical way possible noting that this can vary according to each service provider's individual business model.

Legislative obligations and regulatory requirements must also not create anti-competitive pressures. For instance, some Australian based service providers should not be unduly burdened in comparison to others operating in Australia or overseas-based service providers that are providing similar products and services in the Australian market. The Associations propose that requirements and obligations be defined on the basis of services and customer type and not according to industry participants or a tiered-industry participant model.

The Associations support a workable regulatory framework for ensuring network security and resilience. The framework needs to be adaptable, clear and provide incentives for compliance as well as appropriately allocate shared responsibilities between Government and industry. It should also be equitable, competitively neutral and not costly for industry to implement or comply with.

The Associations agree that the regulatory framework should focus on national security outcomes rather than technical requirements and that industry should be able to demonstrate compliance rather than have prescriptive obligations imposed upon it.

The Associations note that the proposed regulatory framework offers an opportunity to implement formal structures and processes to facilitate improved information sharing and engagement to address perceived threats between Government and industry and that this opportunity is welcomed. This submission includes a proposal to establish a formal vehicle for ongoing dialogue and policy refinement between industry and other security stakeholders, including the AGD, the Department of Broadband, Communications and the Digital Economy, and the Australian Communications and Media Authority (ACMA).

1. Introduction

The Associations

1.1 The Australian Mobile Telecommunications Association (AMTA) is the peak industry body representing Australia's mobile telecommunications industry. Its mission is to promote an environmentally, socially and economically responsible, successful and sustainable mobile telecommunications industry in Australia, with members including the mobile Carriage Service Providers (CSPs), handset manufacturers, network equipment suppliers, retail outlets and other suppliers to the industry. For more details about AMTA, see http://www.amta.org.au.

1.2 Communications Alliance is the primary telecommunications industry body in Australia. Its membership is drawn from a wide cross-section of the communications industry, carriers, carriage and internet service providers, content providers, search engines, equipment vendors, IT companies, consultants and business groups. Its vision is to provide a unified voice for the telecommunications industry and to lead it into the next generation of converging networks, technologies and services. The prime mission of Communications Alliance is to promote the growth of the Australian communications industry and the protection of consumer interests by fostering the highest standards of business ethics and behaviour through industry self-governance. For more details about Communications Alliance, see http://www.commsalliance.com.au.

1.3 The Associations welcome the opportunity to respond to the Discussion Paper, *Equipping Australia Against Emerging and Evolving Threats* (the Discussion Paper) and the Terms of Reference (ToR) for the Parliamentary Joint Committee on Intelligence and Security (PJCIS) *Inquiry into Potential Reforms of National Security Legislation*.

1.4 The Associations support the Government's commitment to protecting the national security of Australia within the challenging world environment of the 21st century and agree that review of the existing legislative framework covering issues of law enforcement, intelligence gathering and national security, including interception powers, is appropriate. In making this submission the Associations note that the Inquiry and its ToR are very broad in scope and that the Discussion Paper outlines significant reforms to the existing legislative and regulatory framework. This will require that there be due consideration by the PJCIS, particularly when it comes to defining the detail around implementation of any necessary changes, as well as a thorough consultation process with relevant stakeholders.

1.5 The Associations have made detailed comments on the ToR and each section of the Discussion Paper in the following sections of this submission.

2. Terms of Reference – The Need for a Principled Approach

2.1 While the ToR requires the PJCIS to have regard to certain objectives, the Associations believe that it may be helpful to agree on some fundamental principles that should underpin any review of the legislation.

2.2 The Associations suggest the following fundamental principles be considered by the PJCIS:

- National security is a concern for all Australians and brings shared responsibilities to the Government and industry alike. Legislation intended to protect Australia's national security must be clear, consistent and workable, without imposing unreasonable obligations or costs on industry.

- Intelligence, security and law enforcement agencies need to be equipped with the appropriate technical resources and skills to effectively manage any threats to Australia.

- Trust and confidence are the key milestones for citizens, end-users and organisations in the digital era. The privacy of individuals, including their communications, should be respected and protected by both the Government and telecommunications service providers.

  NB Principle 1 of the Convergence Review:

  "Citizens and organizations should be able to communicate freely, and where regulation is required, it should be the minimum needed to achieve a clear public purpose"

  The Associations suggest that a corollary of the ability to communicate freely, is the understanding that an individual's communications should generally be presumed to be private and not be subject to interference or interception.

- Lawful interception, including access to the content of any form of communication as well as to the transactional detail of communications and online activities, although recognised as an important tool, must be subject to appropriate checks and balances and its use must be proportionate to the threat, risk or unlawful action.

- Network security and resilience are important in the digital age. A closer level of cooperation between operators and government/agencies is necessary for exchange of information and the identification of possible threats.

- The need to protect critical infrastructure in order to ensure Australia's economic and social well-being is important but the regulatory framework must not impose unreasonable costs or prescriptive and onerous obligations on industry that are disproportionate to the risks involved. Industry is naturally predisposed to protecting its infrastructure without the need for any additional incentives.

- Telecommunications service providers should not be required to create or retain communications data that would not normally be used in the day-to-day business operations or network traffic management requirements of the service provider.

- Costs will necessarily be imposed on telecommunications service providers in the course of assisting law enforcement and national intelligence and security agencies. These real costs must be minimised so that unnecessary costs are not passed onto consumers and do not result in a less internationally competitive Australian telecommunications sector either domestically or on international terms. The economic costs relating to the provision of assistance must be recoverable from the agencies that benefit from such assistance.

3. Interception and the TIA Act

The legislation's privacy protection objective

3.1 The Associations agree a privacy focused objects clause could clarify the privacy principle underpinning the legislation and that such a clause could aid in the interpretation of the Telecommunications (Interception and Access) Act 1979 (TIA Act), although until industry sees a draft clause it is difficult to provide substantive comments.

3.2 The Associations note that it is desirable to have consistency between the Privacy Act 1988, the National Privacy Principles, Part 13 of the Telecommunications Act (Telco Act) and the TIA Act. Consistency is one element in providing telecommunications providers with the requisite certainty they need to know that they are protecting customer privacy while also complying with legislative requirements to provide assistance to law enforcement, intelligence and security agencies. It is preferable for the legislative framework to make clear the balance between privacy and the provision of assistance to agencies so that industry has certainty of its obligations in respect to privacy and security obligations.

3.3 The Associations also believe that community expectations since the legislation was first enacted have not changed significantly. That is, the presumption is still that communications are private and that lawful interception or access to the content or other information about such communications is the exception and is allowed only under certain circumstances defined in the relevant legislation.

Reducing the number of agencies eligible to access communications information

3.4 The Associations believe that rather than looking to define the number of agencies that are eligible to access communications information (that being content and transactional data), a preferred approach should be to reserve access to communications information solely for purposes of addressing instances of serious crime or threats to national security. The nature of the crime/threat in each instance would then determine the type of information required, and the agency/agencies who are eligible to obtain access. If this approach is taken it will be important to be clear about what constitutes 'serious crime'.

3.5 The Associations suggest that the PJCIS and AGD consider the establishment of a facility or process that would enable the secure exchange of electronic information between telecommunications providers and all telecommunications security stakeholder agencies.

Modernise the cost sharing framework: by aligning industry interception assistance with industry regulatory policy and by clarifying the ACMA's regulatory and enforcement role

3.6 The Associations are unsure of exactly what is meant by 'modernise' the cost sharing framework. Without the substance of the proposed changes to the cost sharing framework it is difficult to provide comments. The Associations note that two separate and distinct issues must be considered:

a. What regulations are required to overcome the inherent lack of market incentive to assist law enforcement agencies?; and

b. What is the appropriate cost allocation framework?

3.7 Industry also notes that a number of proposals are listed for further consideration by Government, such as Data Retention and revised Interception obligations. The cost implications of these proposals have not been fully investigated, however preliminary estimates for data retention put the costs in the range of tens to hundreds of millions of dollars. The implications of any proposals to "modernise" the cost sharing framework must be assessed in the context of these proposed reforms representing an expansion to the existing regulatory obligations.

3.8 The Government's policy in relation to "Who should pay cost recovery charges?" reads as follows:

"Users of the Australian Government's information products being cost recovered or individuals/groups that have created the need for regulation should pay cost recovery charges."[3]

Consistent with the same policy, industry's view is that agencies should pay the cost recovery where it is law enforcement and national security agencies that are requesting regulations that mandate the supply of interception and related services.

3.9 The Associations note that there is an implicit assumption in the Discussion Paper that many of the costs of compliance with the proposed legislative and regulatory changes will shift from Government to industry.

3.10 The current framework allocates the cost of interception capability to individual carriers and carriage service providers on the basis that it supports an objective of minimum net overall cost to the community. Alternative mechanisms to achieve this end, for example, a maximum 'best practice' price, could achieve the same end and retain the principle that the seekers of interception and related services should bear the costs of supply. Proposals to alter the current framework motivated by the desire to shift rather than reduce overall costs should be rejected; as should proposals on simplistic but misguided perceptions regarding industry's 'capacity to pay'. On the other hand, if parties requesting the imposition of additional interception and related services are to bear a significant portion of the costs involved, this will incent agencies to consider costs and benefits while also acting as a brake to minimising requests for such services.

3.11 The Associations suggest that for each of the proposed changes to legislative and regulatory requirements, a full cost-benefit analysis needs to be done. Any assumption that industry will bear some or all of the costs involved will result in a flawed analysis if Government is not in a position to fully account for the significant costs that would be borne by industry and inevitably passed onto consumers and shareholders.

[3] Australian Government Cost Recovery Guidelines, July 2005
FINANCIAL MANAGEMENT GUIDANCE NO.4

3.12 The Associations submit that a review of the current model for determining the total cost to be recovered must be undertaken to achieve an acceptable outcome going forward, and suggests that the most efficient cost arrangement for compliance with law enforcement requests is the payment of economic cost. When a service provider is requested to comply with a law enforcement request, that company and its shareholders incur an economic cost to meet the request, as well as the opportunity cost of diverting resources from the alternative purpose to which they would have otherwise been applied. Any alternative use must be real. This is also the real cost to each service provider to achieve compliance that necessitates that there be a diversion of business and operational resources to less productive purposes.

3.13 Implementation of a principle of shared responsibility would go some way towards relieving industry of having to bear the sole burden of the technical and privacy implications of storing data for non-business purposes for the purposes of supplying a service to Government agencies. If the Government is not in a position to bear some of this operational burden then reimbursement of the subsequent cost to industry would appear to be appropriate.

3.14 The Associations question the appropriateness of the ACMA's role as a dispute resolution mediator understanding that a number of parts of the Telco Act were transferred to the TIA Act on recommendations of the Blunn Review. The Associations see this role being fulfilled by an independent judicial organisation, body or individual that has the required experience and technical expertise to provide oversight.

3.15 The Associations also see a role for a formalised government information sharing mechanism, replacing the proposed requirement for reporting mandates, where confidential information can be provided by governments to service providers and vice-versa via a centralised 'clearing house', with access appropriately controlled. Ideally this role would sit within the brief of the AGD, rather than the ACMA. This mechanism should focus on achieving a desired set of outcomes, as opposed to specifying the methodology by which those outcomes are achieved. The Associations table for consideration the development of a set of industry guideline which could serve to achieve this purpose.

Creating a single warrant with multiple TI powers

3.16 While a single warrant with multiple TI powers has the potential to simplify processes from an agency perspective it will shift obligations and due diligence work onto telecommunications providers, making compliance more complicated, less efficient and would result in extended response times.

3.17 The Associations believe that AGD needs to provide more detail about this proposal and explain how the proposal can be justified in terms of potential privacy risks and the shifting of obligations onto service providers.

3.18 A telecommunications service provider must be able to clearly determine from the warrant which services should be intercepted in order to properly implement a warrant. For these same reasons the responsibility to identify relevant services should rest with the intercepting agency and not the service provider. Industry also expects that there will be a continuing need for independent oversight of warrant applications prior to them being served on a carrier or carriage service provider. It would not be possible for the oversight process to fully assess the impact of each warrant if the carrier or service provider is subsequently required to make the decisions about what particular services are to be intercepted.

Implementing detailed requirements for industry interception obligations

3.19 Again, without knowing the substance of the 'detailed requirements' it is difficult for industry to understand the underlying problems that this proposal attempts to address, or to consider whether any alternative strategies exist. Industry is conscious that similar sounding proposals have been raised in the past and have not been pursued due to the potential for significant adverse impacts. We also note that there has been no evidence put forward to justify detailed requirements.

3.20 The Associations see value in high level set of requirements for industry interception obligations to be clear, straightforward and reasonable. This provides sufficient certainty in outcomes for Agencies while allowing industry to meet its obligations in the most efficient and economical way possible.

3.21 This key risk with any legislated 'detailed requirements' is that it is overly prescriptive and likely to become more onerous and less effective in the face of future development in the telecommunications industry. 'Australian only' obligations will substantially drive up initial and ongoing costs, limit the range of services that may be offered as well as the selection of vendors, and delay the rollout of new and upgraded services. The Australian market represents a tiny percentage of the global market and some vendors may simply refuse to make Australian specific products, while others may relegate Australian production to a lower priority and apply longer development timetables. Withdrawal of vendors from the Australian market would have the consequential effect of reducing price tension during tendering processes.

3.22 Industry's view is that a more appropriate action would be for AGD to influence the development of international standards so that vendor solutions will better meet Australian requirements. Industry's understanding is that AGD has been resourced to participate in the relevant international standards processes and has been doing that work for a number of years.

Extending the regulatory regime to ancillary service providers not currently covered by the legislation

3.23 This proposal indicates that interception-type obligations could be extended beyond Australian based service providers to include website /application providers, such as social media operators, webmail services and cloud computing providers. Another effect of this extension to Australian service providers would be that any products that the service provider was offering that covered these types of services, (e.g. webmail or OTT (Over-The-Top) applications), not previously subject to lawful Interception obligations other than for the carriage element, would also be caught. The Associations note that this push to include ancillary services would appear to be at odds with the tiered approach proposed in the same discussion paper.

3.24 There is no discussion accompanying the proposal to indicate how the regulatory regime would apply to global service providers located outside of Australia. For the proposal to have any substantial impact, industry expects that the following matters need to be addressed:

- Jurisdictional coverage of Australian legislation;
- Established and potential mechanisms for international cooperation;
- Identification of end users of such services; and
- Ongoing competitiveness of Australian based service providers.

Implement a three-tiered industry participation model

3.25 Industry favours a tiered participation model, where investment in interception capabilities is based on Agency need and risk, as opposed to the current blanket obligation which requires the deployment of interception capabilities that in some cases are unlikely to be used. Large scale aggregate services, for example, the access connections to Government and corporate networks are likely to be of low intrinsic interest to Law Enforcement and National Security Agencies. Further, the communications of any particular individual within such aggregated access services cannot be separately identified by the service provider. For these reasons such services should be exempted from the requirement to supply interception.

3.26 The proposed model of tiered participation based on participant status opens up the possibility of significant bypass of interception capabilities and requirements. A regulatory regime that clearly signals that small service providers will have no interception capabilities invites organised criminals and terrorists to use such small service providers. A more effective regime would be to focus the supply of interception capabilities on mass market and access services where interception is most likely to be utilised and be more effective.

3.27 Any future model should be based on a risk management approach, rather than a risk elimination approach, as currently applies. In this regard, industry is mindful that other investigative tools, including surveillance techniques, are acknowledged and accepted as being less than 100% effective. Industry's view is that any future interception regime should recognise that no system can achieve perfect coverage all of the time and should instead focus on achieving reasonable outcomes for reasonable levels of national investment.

3.28 As the industry moves away from traditional voice telephony to IP based services and applications to deliver communications, there are a range of issues that apply to the retention/maintenance of traffic data. The Associations believe that it is the content itself, manifested through a wide range of services that requires greater scrutiny by agencies, with a reduced focus on the participants in the delivery chain. Industry's view is that a risk management approach should also be applied across any proposed data retention regime.

3.29 The Associations note that while this content delivery layer is one that may be of greater interest to agencies, the global supply of such services also raises a number of associated jurisdictional issues.

3.30 The current blanket approach of the TIA Act potentially gives rise to replication of interception capabilities at the carrier, wholesale service provider, retail Broadband service provider and application service layer. A more efficient regulatory framework should be sought, where replication of interception capabilities is not required.

Establish an offence for failure to assist in decryption of communications

3.31 The Associations note that failure to assist in the decryption of communications data has not warranted any form of obligation or mandatory compliance in the past. Clarification is therefore sought as to why there is now a proposal to establish an offence for failure to assist, and what type of behaviour or activity the Government is wanting to address.

3.32 In addition, the discussion paper does not specify the parties to which the proposed decryption assistance obligation is to apply. End users, wholesale service providers, broadband retail service providers and content providers could all potentially play a role in the encryption of communications. Where the provider is based offshore then the matter of jurisdiction also needs to be considered.

3.33 Any decryption requirement should also specify that the obligation is to make available, if it is available, the means for decryption, as opposed to the actual content/communications that is to be decrypted.

3.34 There must not be a presumption that a person or organisation is capable of decrypting communications. The imposition of sanctions or penalties must be based on proof that the person or organisation is capable of assisting with the decryption of communications and there is evidence they have refused to do so.

Institute industry response timelines

3.35 The Associations acknowledge the benefits of providing timely access to communications data from a security consideration, but note that the existing 'reasonably necessary assistance' requirement allows providers to determine their own response times, determined by CSP processes and costs in meeting such requests. If industry is to be asked to meet specified response timelines, a minimum level of automation will need to be built into industry's existing data provision processes to accommodate the Government's requirements. Automation of these processes will come at a cost to industry and agencies and the Associations believe it is reasonable that this cost should be reimbursed by the Government.

3.36 Prescribing industry response timelines will inevitably increase industry costs that will need to be weighed against any perceived benefits. For these same reasons charges should be able to be conferred back to agencies that are benefiting under such arrangements.

3.37 Any standards for industry response times would also need to be proportionate to the volume and risk associated with particular services and service providers. Applying standards for industry response times across the industry could lead to overall increased costs but not overall increase in benefits. Mandated response times could only be met by process automation across the industry. This would require investment in process automation, with facilities required across all service providers, large and small. But substantive benefits are unlikely to be realised at the smaller providers, where requests are typically low volume and infrequent.

3.38 Industry's view is that the current regime enables the Law Enforcement and National Security Agencies to negotiate service levels for the supply of reasonably necessary assistance. Further, Association members are not aware of any substantive difficulties with current levels of responsiveness to agency requests.

3.39 A more appropriate direction would be for industry and agencies to work cooperatively in achieving higher levels of automation of warrant and data request processing.

3.40 Industry's view is that there are sufficient powers within the current regulatory regime to deal with any provider that does not provide reasonably necessary assistance to Agencies. Should it be necessary, the reasonableness of any response timeframes is able to be assessed by Regulators on a case by case basis.

Applying tailored date retention periods for up to 2 years for parts of a data set, with specific timeframes taking into account agency priorities and privacy and cost impacts

3.41 The Associations' view is that the Government has not provided sufficient justification for the implementation of data retention. In particular there appears to have been no proper assessment of the relationship to be derived and the costs (social and financial) involved in implementing such a regime.

3.42 One of the propositions put is that service developments and increased globalisation have limited the effectiveness of interception. Current and future industry structure clearly indicates that a data retention regime will be subject to the same limitations on effectiveness and determined users will continue to have ready means to disguise their identities and their communications.

3.43 Further, the Associations consider that the existing provisions obliging carriers and service providers to supply 'reasonably necessary assistance' provide adequate scope for Agencies to obtain data.

3.44 The Associations have serious concerns relating to the specific proposal that would allow "tailored data retention periods for up to 2 years for parts of a data set". For purposes of establishing precedence, the Associations draw attention to the European Commission's Evaluation report on the Data Retention Directive, April 2011, which found that most data requested by enforcement agencies was less than 6 months old. The Report further states that "Quantitative evidence provided so far by Member States regarding the age of retained data suggests that around 90% of the data is six months old or less, and around 70% three months old or less when the (initial) request for access is made by law enforcement authorities."[4]

3.45 The European Commission's Report also notes that in some countries (Finland, the UK) providers are reimbursed the capital and operational costs that are incurred in complying with the respective Data Retention regimes. Similarly, the Associations also believe that the full cost of complying with an Australian data retention regime should be borne by the Federal Government.

---

[4] 2011 European Commission's Evaluation report on the Data Retention Directive

3.46 Service providers have previously put forward their views to the AGD on both cost sharing arrangements and models for retaining data. The cost sharing arrangement favoured by service providers is that currently in place in the UK.[5] The cost of a data retention capability is borne fully by the UK Government and has acknowledged the value of data in assisting the Home Office efforts in fighting crime and terrorist activities. The UK has a system of voluntary[6] data retention where service providers retain some data under agreed arrangement with the UK Home Office.

3.47 To this point clear boundaries around requests for additional data have not been established in any of the conversations on the data retention issue. In terms of setup costs industry estimates place the cost of capture and retention at close to one hundred million dollars. If the source and destination IP addresses were to be included in the capture and retain requirement the setup costs would be likely to approach a figure in the region of five hundred to seven hundred million dollars ($500 million - $700 million). The inclusion of a single additional data element has the potential to increase the capture and retention cost by tens of millions of dollars. More accurate costing could be made available by industry upon provision by the AGD of details of the actual data elements to be included in a data retention regime.

3.48 The Associations contend that costs of this magnitude would appear to warrant scrutiny at a parliamentary level, as opposed to an agency/AGD level. This would also enable the privacy implications of each additional data element to be assessed. Consider, for example, the inclusion of a requirement to capture and retain the location of mobile customers, as has been proposed as part of the DBCDE IPND review. With the addition of a data retention obligation, this could be expanded into an ongoing surveillance regime capable of tracking the movements of all mobile customers.

3.49 The Associations also believe that the Government should accept full responsibility and liability, including costs, for storage of the retained data. The Associations believe that requiring industry to store retained data would be asking the private sector to assume risks and liabilities that more appropriately should rest with Government.

3.50 The Associations are also seeking for Government to be clear about the extent to which any data retention obligation could be utilised in the future to require industry to create or capture information that is not used for normal business purposes, noting that this would conflict with the privacy principle that telecommunications providers should not be required to create or store data when it is not necessary for normal business purposes.

3.51 Consideration also needs to be given to the changing nature of telecommunications traffic and the subsequent increase in use of services (though not necessarily captured and retained). As the Discussion Paper states, data traffic has experienced exponential growth over the last several years and this is only expected to continue over coming years. In addition, some major service providers have begun to utilise Network Address Translation equipment in their networks to deal with the runout of IP address capacity. Such equipment can generate in the order of 40 Billion records per day in a single application within a single provider's network.[7]

[5] http://www.legislation.gov.uk/ukdsi/2009/9780111473894/contents

[6] http://www.legislation.gov.uk/uksi/2009/859/pdfs/uksiem_20090859_en.pdf

[7] Source: Optus

3.52 The massive data volumes involved will make it practically difficult to search data in a short timeframe. This would be at odds with other proposals to mandate industry response times.

3.53 The ACMA's Communications Report 2010-11 provides figures which substantiate this predicted future growth in data traffic[8]:

- As at June 2011, there were 29.28 million active mobile (voice and data) services, representing an increase of 13% on the previous 12 month period.
- As at June 2011, there were 10.9 million internet service subscribers, representing an increase of 15% on the previous 12 month period.
- Up to the quarter ending June 2011, the total (dial-up plus Fixed broadband plus Wireless broadband) volume of data downloaded was 274 202 Terabytes, representing an increase of 76% on the previous 12 month period.

3.54 Some concerns about a data retention regime that the Associations have raised in previous consultations are as follows:

3.54.1 Industry is particularly concerned that a 'Data Retention' obligation has the potential to create an additional requirement to capture new data, retained for reasons outside the original business purpose, and to be presented at a later date, in an altered format;

3.54.2 The financial cost is only one element of the total costs of this regime. There is likely to be some additional social cost, constituting both the cost of loss of privacy and a further additional risk to security as the retained data becomes itself a target for unlawful access. Industry believes it is generally better for consumers that service providers retain the least amount of telecommunications information necessary to provision, maintain and bill for services (including calls and transmissions);

3.54.3 Consideration should also be given to the potential interaction of this proposal and existing legislation that enables third parties with access to data by way of subpoena, search warrant and any other lawful request process There would need to be additional provisions requiring that material retained under this regime not be made available to parties other than defined national security and law enforcement agencies and only then for the purposes of 'serious crime or national security';

3.54.4 Industry is of the view that data should only be retained where such data is generated by or associated with a service supplied by a given provider. In addition providers of wholesale or transit Internet services should not bear the obligation to retain data generated by end-users served by retail Internet service providers (the customers of those wholesale or transit Internet services). The Association's position is that data needs be captured once only, not at every layer in the service delivery process;

[8] ACMA's Communications Report 2010-11

3.54.5 Industry requires that any data retention legislation must also contain a caveat which expands upon the current concept of immunity to incorporate acting in good faith, and provide immunity to the reporting obligations under the Privacy Act; and

3.54.6 Regarding storage of any data that is required to be retained, the Associations position is that Government be responsible and accept all liability (including costs) for storage.

4. Telecommunications Security Sector Reform – Telco Act

- ***Amend Telco Act to address security and resilience risks posed by the telco sector***

- ***Institute obligations on industry to protect networks from unauthorised interference***

- ***Obligations to provide Govt with info on significant business and procurement decisions and network design***

- ***Targeted powers for Govt to mitigate and remediate security risks with the costs to be borne by providers***

- ***Creating appropriate enforcement powers and pecuniary penalties***

4.1 The Associations agree that the regulatory framework should focus on security outcomes rather than technical requirements and that industry should be able to demonstrate compliance rather than have prescriptive obligations imposed.

4.2 Noting the importance of network security and resiliency in the digital age, the Associations on the whole welcomes the Government's pragmatic security outcomes/objectives based approach as opposed to stipulating a requirement for Government approval of network architecture at a technical or engineering level.

4.3 Close cooperation between service providers and Government is necessary for exchange of information and possible threats observed. Nonetheless security and resiliency policy should be based on approved international standards. Security is an important milestone but should not slow down infrastructure deployment that it requires in Australia.

4.4 The Associations understand the Government's objective to protect the security of telecommunications networks from unauthorised interference. However, the Associations are not convinced that the consultative process has to date identified a workable model for an appropriate regulatory framework.

4.5 A regulatory regime that mandates external controls over procurement and network design practices and requires extensive notification practices would certainly amount to an overly prescriptive level of intervention. The Associations believe that such a regulatory framework would restrict the ability of network and infrastructure providers to cost-effectively implement platforms that are innovative, progressive and provide supplier differentiation. Controls over procurement would also unnecessarily increase timeframes for network rollouts, which would contradict the Government's advocacy for increased broadband deployment.

4.6 Industry has already outlined its position in its submission in response to the AGD discussion paper *"Proposed regulatory scheme to enhance the security, integrity and resilience of Australia's telecommunications infrastructure",* industry's view is that any measures should apply only to 'critical infrastructure', where the definition of this term should be agreed upon through consultation with industry. In contrast the proposed model appears to lack any level of transparency and may result in agencies dictating the form of private sector network deployments without requiring agencies to disclose their decisions. Accordingly, the Associations have proposed that requirements regarding networks and infrastructure need to be clearly defined so that industry can invest and deploy infrastructure with confidence and, without concern that government will raise objections once such networks are deployed.

4.7 Should the Government decide to proceed with the model proposed in the Discussion Paper, the Associations propose that it should include a facility for an appropriate and truly independent means of review or appeal to prevent arbitrary or unjust use of directions or penalties. The Associations suggest that there could be a role for an adjudicating or mediating body that would be able to intervene when Agencies and service providers are not able to agree on the risks to network or infrastructure security.

4.8 Concerns previously raised by the Associations on the proposal to make legislative and regulatory changes to enhance the security and resilience of telecommunications network infrastructure, are as follows:

4.8.1 the potential for the proposed regime to bring providers into conflict with existing corporate regulations, particularly those relating to the disclosure of information;

4.8.2 the compatibility of the proposed regime with existing corporate governance where a provider's activities might be driven by decisions made outside of Australia. Many operators have global or regional supply arrangements which would in effect become invalid under the proposed regime. This would result in costs to operators in the amount of many millions of dollars as a result of having to break regional/global supply contracts;

4.8.3 impacts on competition in the market-place and risk that proposed requirements may create a barrier to entry for new, lower cost providers and could eliminate some of those already in the market, resulting in decreased market competition on pricing and general consumer detriment;

4.8.4 the absence, to date, of any protection/indemnity to civil action for providers who have acted in good faith under the requirements of the proposed amendments;

4.8.5 the fact that the rapidly changing technology landscape, where potential vulnerabilities now exist at the physical, network and application layers, has not been sufficiently taken into account, specifically with regards to the concept of 'critical infrastructure'; and

4.8.6 the need to engage further with industry on possible regulatory alternatives: such as a set of guidelines to provide guidance for providers in the areas of procurement and network design; a process for

Government-industry engagement where a high risk event is identified and a framework for periodic reporting to Government agencies on the security measures being taken by providers.

4.9 The Associations support a regulatory framework that is adaptable, transparent, provides incentives for compliance, shares responsibility, is equitable and competitively neutral and is not costly for industry to implement or comply with.

4.10 Initiatives developed through deep and solution-oriented consultation with industry and government are the preferred approach for reaching practicable solutions on security issues. The Associations accordingly propose the establishment of a formal means of engagement with telecommunications security stakeholders to further refine any legislative proposals during the period of the Committee's deliberations and/or in the wake of the Committee's report.

4.11 The existing AGD Experts Group would appear to be the logical vehicle for this engagement, noting that its membership contains representation from the key telecommunications security stakeholders. The Experts Group could be convened following the Committee's receipt of the AGD submissions on this inquiry and could continue its work on these issues after receiving the guidance flowing from the Report of the Committee's Inquiry.

4.12 With regard to the proposal for an amendment to the Act to allow for the creation of appropriate enforcement powers and associated pecuniary penalties, the Associations position is that development of a financial penalties framework is premature, and not conducive to the development of an appropriate level of trust, and a common vision on security and resiliency, between Government and service providers. All stakeholders should be part of the process of defining both methodology and objectives.

4.13 An alternative, and preferable, approach would be to require a reporting regime relating to cyber-attacks on Australian networks with noticeable operational impact by service providers as opposed to a system which enforces penalties on those providers. Where service providers can demonstrate implementation of reasonable minimum network security measures then imposition of a penalty based instrument would seem to be punishing those service providers who have taken steps to ensure, within their control, that a certain level of precaution has been exercised at a network level.

5. ASIO Act and ASIO's Warrant Provisions

Update definition of computer

5.1 Any updated definition of computer should include wireless or hand held devices that have a facility for accessing, downloading and transmitting communications data. The role of computer networks also needs to be given consideration.

Establish named person warrants

5.2 As noted previously in this submission, in order to properly implement a warrant a service provider must be able to clearly determine from the warrant what services should be intercepted. The onus to identify relevant services should rest with the intercepting agency, and not require any level of interpretation on the part of the service provider. Clarity of detail in a warrant will also facilitate a timelier response from providers, noting this is another objective of the Government's proposal.

Enable disruption of a target computer

5.3 Disruption of a target computer, or network, should be facilitated by agency mechanisms. Industry would strongly oppose any proposal for disruption mechanisms being inserted into information communications networks, communications devices, and any other publicly available applications platforms.

ASIO's ability to co-operate with the private sector

5.4 A cooperative engagement framework that takes into account the varying security responsibilities of end users, service providers and agencies, is highly desirable. Where two or more service providers may be required to cooperate for non-business purposes, e.g., taking action to identify, or minimise, a potential security threat, some level of indemnification against other overarching regulations (like the Australian Consumer Law, the Privacy Act and Part 13 of the Telecommunications Act), should be afforded to service providers where such cooperation may be warranted.

6. Conclusion

The Associations look forward to continued engagement in the PJCIS review's consultation process and would welcome the opportunity to discuss, in greater detail, the proposal to engage with the Committee via the Experts Group, and how the feedback provided in this submission could be expanded upon to include detailed solutions to the issues highlighted in the Committee's discussion paper.