COMMUNICATIONS ALLIANCE LTD
www.commsalliance.com.au

AMTA
Australian Mobile Telecommunications Association

Submission:

Senate Legal and Constitutional Affairs References Committee

Inquiry into 'Comprehensive Revision of Telecommunications (Interception and Access) Act 1979'

27 February 2014

Introduction

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 www.amta.org.au.

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 www.commsalliance.com.au.

Communications and AMTA (the Associations) welcome the invitation to provide comments on the Terms of Reference for its Inquiry into a comprehensive review of the *Telecommunications Interception and Access Act 1979* (the Act).

The Associations have provided some general comments about the review of the Act as well as more specific comments on some of the recommendations cited in the Terms of Reference.

Review of the Act

The telecommunications industry has a long history of co-operation and partnership with the relevant Government and Law Enforcement and National Security Agencies (LENSAs) with regard to the provision of interception capabilities and assistance to law enforcement under the obligations of the Act. An approach based on the partnership between industry and LENSAs should form the foundation for a revised Act.

The Associations recognise the Government's commitment to protecting the national security of Australia within the challenging world environment of the 21st century. Intelligence, security and law enforcement agencies need to be equipped with the appropriate technical resources and skills to effectively manage any threats to Australia.

The Associations note that recent high profile security breaches and publicity around Government intelligence and security activities are contributing to community concern about the security of their telecommunications and internet services. The United States and some European countries are now considering the scope of their interception, surveillance and data retention practices and laws.

The Associations also note the Government's deregulation agenda and commitment to reduce unnecessary red-tape and regulatory burden on industry.

In such a context, the Associations agree that a comprehensive review of the Act is timely. A review process that looks to clarify and simplify the requirements of the Act while also reducing regulatory burden and minimising the costs of compliance is welcomed by the Associations.

National security is a concern for all Australians and brings shared responsibilities to the Government, industry and the community. The Act and its supporting regulatory framework must be clear, consistent and workable, without imposing unreasonable obligations or unrecoverable costs on industry.

The Associations strongly believe that lawful interception, including access to the content of communication as well as to the transactional detail of communications and online activities, is an important tool. It must be subject to appropriate checks and balances and its use must be proportionate to the threat, risk or unlawful action.

Further, telecommunications service providers should not be required to create records about customers' use of services that would not otherwise be used in the business operations of the service provider. Any retention of business records should be proportionate to the costs, the sensitivity of the data and the quantified value to LENSA investigations.

Finally, costs are incurred by telecommunications service providers in the course of providing assistance to LENSAs and these costs are in turn borne by consumers. These costs must be minimised so that costs do not become a burden for consumers. Cost burdens on industry also result in a less internationally competitive Australian telecommunications sector. The Associations strongly maintain that the full costs relating to the provision of assistance must be recoverable from the agencies that benefit from such assistance.

The Associations suggest the following principles should guide the objectives and desired outcomes of a review of the revised Act:

- **Obligations should be transparent and designed to build trust among the community regarding law enforcement and national security activities.**

- **The partnership between industry and LENSAs should be encouraged and promoted.** Requirements should be set out in a way that encourages adoption of a partnership approach in meeting obligations.

- **Industry requires certainty of its regulatory obligations.** To provide certainty of regulatory obligations, all obligations on the telecommunications industry should be contained in a single Act and should be clearly defined. The open-ended obligation to provide "reasonably necessary assistance" should be replaced by clearly defined obligations with all expectations and limitations appropriately spelt out.

- **Obligations must be practicable and achievable as well as technology and service neutral.**

- **Costs to industry and LENSAs should be minimised.** Any review should include an evidence-based cost-benefit analysis and there should be a net benefit of any obligations.

- **Costs must be allocated on user-pays basis.** That is, LENSAs who benefit from a requirement or obligation must bear the costs associated with it. This promotes a proper cost-benefit analysis and balancing of benefits to LENSAs versus burden on industry.

- **Obligations placed on industry should mirror and match the powers and authorisations of LENSAs.**

- **Regulations must be flexible (in recognition of a rapidly evolving market and technological ecosystem).** To provide the necessary flexibility, disallowable instruments should be preferred over Ministerial Directions, providing greater transparency and accountability. Proposed changes to instruments should always be subject to review by the Productivity Commission with regard to the principles of best practice regulation. Changes to regulatory instruments should also require public and industry consultation, with the objective being that consensus is achieved before new obligations are imposed.

- **Australian-based suppliers should not be disadvantaged or constrained in how they supply services.** It must be recognised that Australian suppliers increasingly compete alongside global services and also depend on the supply of services, network equipment and customer handsets that are designed and built for a global market.

- **The Act must recognise and adhere to international standards.**

- **The Act should use the ETSI model[1] to define functions relating to interception.** This should replace the current concepts of "delivery point", "delivery capability" and "interception capability" in the current Act.

- **Automation should be promoted.** Automation of carrier and CSP tasks is expected to reduce overall costs and improve the timeliness of support to LENSA's. Automation should be encouraged by allowing all costs of automation to be recovered.

- **Exemption process should be efficient, timely and pragmatic.** The Act should contain defined criteria for evaluation of exemptions.

[1] ETSI is the European Telecommunications Standards Institute. A model for interception and related warrant administration and delivery functions is contained within ETSI ES 201 158.

Red Tape Reduction

The Act and its regulatory framework are overly complex and requirements and obligations on the telecommunications industry can be open-ended and unclear. Such uncertainty can result in excessive costs being incurred both by industry and agencies.

The Associations recommend that in reviewing the Act the Government takes the opportunity to reduce red tape and minimise the regulatory burden on industry. A full cost-benefit analysis should be part of the comprehensive review of the Act.

The Associations maintain that in order to ensure the costs and benefits associated with the provision of assistance to LENSAs by the telecommunications industry are truly taken into account; the entire costs should be borne by and attributed to the LENSAs receiving the benefits. This is in accordance with the principle that persons performing tasks for Government should have their costs met.

Methods for recovering costs incurred by telecommunications service providers must also be streamlined and simplified so that they can be fully recovered and that costs are understood up-front as technical and operational applications are developed. Costs and cost recovery should be based on actual costs incurred to fulfil requirements with a consistent system used to recover costs. Cost recovery should not be subject to complex and time-consuming negotiations.

Finally, the Associations recommend the development of clear guidelines to accompany the revised Act so that telecommunications service providers can have certainty over the extent of their obligations. Guidelines should clearly set out the priority of legislation so that service providers can understand how the Act and its obligations can be complied with in a way that is consistent with the obligations and requirements of Privacy legislation and the many other regulatory requirements imposed on industry. Clear guidelines will also prevent obligations from being broadened over time and provide the requisite regulatory certainty to telecommunications service providers, allowing them to better manage investments.

This would then allow for proper consideration of reasonable requirements in relation to cloud computing and outline these requirements clearly in guidelines to provide industry with certainty around regulatory obligations. For example, in respect to cloud services it is unreasonable for providers, specifically carriers and CSPs, as opposed to non-telecommunications cloud providers, to be subject to preservation requirements under the Act.

Cloud account holders range from individuals to enterprise organisations. The logistics necessary to effectively carry out a preservation request (i.e. capture and maintain every iteration of every file in the customer's cloud account) is an extraordinary and unfair cost burden that would not be equally incurred by all cloud providers, thereby creating a barrier for carriers and CSPs to entry into this market.

Terms of Reference – Comments on Recommendations

PJCIS Recommendations:

Recommendation 3

The Associations believe that opportunities to reduce the reporting burden (sections 306, 306A, 308 of the Telecommunications Act) on industry exist. For example, the requirement to report on information released to the TIO is not required as the TIO already reports on its activities and it is reasonable to expect that a CSP will supply the TIO with information as part of any complaint investigation. There is no value added by this particular record keeping and reporting obligation. The Associations suggest that only reported results that have been demonstrably used in policy decision making over the past two years should be retained.

Recommendation 4

Recent events as well as public and media attention clearly demonstrate that effective accountability is a community expectation. The Associations believe that this accountability could be achieved by direct oversight of LENSAs and their activities, rather than by placing reporting obligations on the telecommunications industry.

The Associations also maintain that it would be useful for telecommunications service providers to have a clear understanding of which agencies are eligible to access communications information. While this does not necessarily mean that the Act should contain a list of eligible agencies, it should limit and define the number of eligible agencies appropriately and definitively. The Associations note that dealing with a multitude of agencies under the current model results in a significant impact on costs as service providers are responsible for vetting requests from agencies that range from those responsible for national security to local councils across the country.

To bring further governance to the process, industry members would prefer requests for preservation of stored communications have greater rigour and structure to the submission by requiring either a senior member of the agency or authorised officer to make these requests.

Recommendation 5

The Associations submit that all LENSAs with access to telecommunications data should pay for the costs incurred by the telecommunications industry in providing data.

Automation of processes should be used to improve efficiencies and cost minimisation as well as enable carriers and CSPs to better handle high volumes of requests for data.

Further, as per the comments above in relation to recommendation 4, clarity around which agencies are eligible to have access to telecommunications data would be useful and streamlining agency access could result in cost efficiencies.

Recommendation 7

The Associations believe that recommendation 7 is unclear as ‘attribute based interception’ has not been fully defined.

While industry understands that more flexibility may be needed in how agencies can issue a warrant, the Associations maintain that any warrant must be clear and provide certainty to service providers regarding which services are included. The onus should not be on the service provider to interpret the warrant or determine which services are included in a warrant.

Further investigation of "attribute based interception" is required in accordance with the principles of best practice regulation to determine:

- The problem that this proposal is seeking to solve. That is, in terms of the current Act it is not clear whether the proposal is seeking to solve a problem with Interception Capability or Delivery Capability or problems at LENSA monitoring centres.
- Whether attribute based interception can be achieved in practice. Practical solutions may require interception of all communications first, followed by filtering based on attributes. The division between Interception Capability and Delivery Capability concepts in the current Act may not be sufficient to define arrangements for attribute based interception.
- The impact on existing interception capability investments of the industry. Will attribute based interception make existing investments in interception and delivery capability obsolete?
- The costs and benefits arising from any attribute based interception capability that would need to be installed across the entire customer base at considerable cost. Are the overall costs justifiable for the incremental benefit that would be obtained by LENSAs?
- Cost attribution. The current obligation on carriers and CSPs to bear the cost of interception capability was justified on the basis that such costs would be incremental to standard network equipment costs. If the solutions for attribute based interception require the deployment of separate interception equipment, the costs will no longer be incremental and cost attribution should return to the basis under previous legislation that carriers/CSPs neither gain nor lose from providing interception capability for use by LENSAs.

Recommendation 8

One of the cost drivers in building interception capabilities is the number of LENSAs that may separately request interception, including a growing number of Law Enforcement Integrity Agencies. The quantity of LENSAs exceeds in some cases the capability of standard interception equipment available from vendors. The opportunity for cost savings across the telecommunications industry and LENSAs through the establishment of shared monitoring systems requires examination.

Recommendation 9

The Associations suggest that this recommendation should be extended as follows:

- The Act should be reframed to control all aspects of lawful access to communications and data held by carriers and CSPs, with reduction in the scope of Part 13 of the Telecommunications Act accordingly. There is currently ambiguity and duplication, for example, between the operation of Part 4 of the Act and section 280 of the Telecommunications Act. To this point, the Associations would appreciate greater clarity or guidance on which Commonwealth Act takes precedent regarding the disclosure of

telecommunications data. Currently, laws are written in such a way that carriers and CSPs can be served with competing legislation from various Commonwealth agencies seeking this data under their own agency's legislation.

- Obligations placed on telecommunications carriers and CSPs to support LENSAs are split between the Telecommunications Act (Part 14) and the Act. Obligations on the telecommunications industry should be removed from the Act and placed back into the Telecommunications Act. This would also remove any perception of a potential conflict of interest the Attorney General's Department may have between balancing policies; extending the powers of LENSAs on the one hand and increasing obligations on industry on the other hand. The Associations suggest that the DoC is better placed to evaluate the overall objectives of the Telecommunications Act before any additional regulatory obligations are placed on the telecommunications industry.

- Part 13 of the Telecommunications Act should be revised to remove obligations already covered by the Privacy Act. In particular, any privacy matters subject to the Privacy Act should not also be subject to any "double jeopardy" investigations, reporting or sanctions under the Telecommunications Act.

Recommendation 10

The Associations believe that there is an opportunity for red- tape reduction under the existing warrant regime. The current Act originally required all warrants to be served on the Managing Director of the company. This was often impractical in a large company and opened the door for defence tactics to challenge evidence on the basis of administrative process. The legislative amendment that addressed this point added further bureaucracy for carriers and CSPs yet it failed to adequately recognise that the major carriers, where most of the interceptions take place, operate Law Enforcement Liaison Units. Reference to internal carrier/CSP processes and procedures should be minimised to avoid the risk of defence tactics to challenge evidence on the basis of the internal carrier/CSP administration of Agency support functions.

The Associations suggest that if any carrier/CSP warrant processes and associated evidentiary certificate processes need to be defined, it should be done in subordinate instruments, not primary legislation, so that issues associated with the evidence process can be dealt with more effectively and timely.

Recommendation 11

The obligations contained in subsections 313 (1) (2) (3) and (4) of the Telecommunications Act are open to wide interpretation. This has resulted in some carriers and CSPs being concerned that they may breach these obligations if they do not comply with *all* agency requests for information and content, even if such requests require the commitment of resources beyond the obligations of the Act and beyond the capabilities of approved Interception Capability Plans. These sections should be amended to clearly define and detail the obligations imposed on industry and align obligations with the specific access powers vested in LENSAs by the Act.

Further, mobile service providers have been subject to additional costly and ineffective regulations governing the supply of prepaid mobile services. The Associations strongly believe that these regulations are ineffective in meeting their objective as they are based on the assumption that criminals (or persons of interest) will always supply their true identity to their mobile service provider. However, identity can, in fact, be easily and effectively concealed through secondary trading in services and ID theft. The Prepaid ID check regulations do not meet the fundamentals of Best Practice regulation as they are incapable of meeting their objective and have not demonstrated that the benefits of the regulations outweigh the costs. The regulations inconvenience consumers, burden industry and do not achieve their stated purpose. Further, no cost recovery arrangements have been established despite the fact that there is no business requirement for performing ID checks for prepaid services, making this obligation solely for the benefit of LENSAs.

Further, lack of certainty around the Interception Capability Plan (ICP) process means that despite having an approved ICP, demands for the installation of costly additional capabilities can be received on an ad-hoc basis. In an environment where capital budgets are tightly constrained, this can lead to disruption of capital investment programs and delayed roll out of additional mobile network coverage.

Finally, despite the cost recovery principles in the Act and Telecommunications Act, it is extremely difficult to recover the full cost of providing assistance to Agencies due to the following reasons:

- Call costs associated with delivery of telephone intercepts cannot be billed from standard billing systems whilst maintaining the secrecy needed for the numbers of the Agency monitoring centres. It is uneconomic to build a separate secure billing system for this purpose, so these costs are simply not recovered.
- Cost recovery for Delivery Capability is generally at around 50% of actual costs incurred. The contracting Agency insists that warrant provisioning processes are part of Interception Capability. However, in practice it is infeasible to install a Delivery Capability without an associated warrant provisioning process. Without a Delivery Capability, LENSAs would be required to pay for manual warrant provisioning. Despite the Agencies obtaining improved warrant provisioning times, industry is left bearing the cost of 50% of Delivery Capability because of the contracting LENSA's hard line interpretation of the associated warrant provisioning functions.
- Cost recovery for Delivery Capability is all too often delayed by complex legal arguments associated with establishing formal contracts. Whilst there is no mention of contracts in the Act, the lead Agency, ASIO, insists on establishing contracts before any cost recovery can occur. The contract process has then also been used to attempt to extend the obligations on individual CSPs through the inclusion of terms and conditions above and beyond those required for compliance with the Act. Limited carrier/CSP capital is tied up while these contract negotiations drag on.

The current Act replicates interception capability obligations across multiple organisations involved in the supply chain that could include, for example, a carrier, a wholesale network operator, a wholesale service provider and a retail service provider. This results in costly and wasteful replication of interception capability resources. An alternative, for example, would be for NBN Co to

supply a common interception capability to meet the needs of Agencies and relieve all downstream CSPs from having to invest in interception capabilities and associated delivery capabilities. Placing the responsibility for funding interception capabilities on the requesting Agencies will better focus their attention on achieving value for money, reduction in wasteful duplication, prioritisation of investments and the removal of inefficient contracting processes.

Where cost recovery arrangements are still required, they should be based on simpler processes:

- an agreed scope of works,
- submission of invoices detailing use of internal Telco resources and receipts for vendor supplied equipment and associated actions to achieve the agreed scope of works,
- prompt payment back to the carrier/CSP.

Recommendation 12

Regulatory enforcement action undertaken by the ACMA should be confined to carriers or CSPs that have consistently refused to cooperate with the LENSAs. Matters of dispute between the industry and LENSAs about specific aspects of interception or assistance arrangements should be referred to an independent expert arbiter appointed via a commercial alternate dispute resolution service.

Recommendation 13

See comments regarding recommendation 11 above.

Recommendation 14

The Associations are not sure what is meant by the term “ancillary service provider”. The Associations note that organisations mentioned in the PJCIS report, including, Facebook, Twitter and Google are not carriers or CSPs as defined in the Telecommunications Act. Such organisations are therefore not subject to the Act or Part 13 of the Telecommunications Act. The term “ancillary service provider” is not defined in the existing legislation.

The obligations in the current Act do not apply to content service providers. The Associations question if this recommendation is actually a suggestion that obligations be extended to content service providers, noting that the implications of this would warrant close consideration around the benefits and costs involved. The Associations submit that content service activities of carrier/CSPs should not be subject to interception and related obligations that do not apply to distinct content service providers. As per comments with regard to Recommendation 11 above, there is a significant risk that obligations placed on “ancillary service providers” will simply add another layer of replication of interception capabilities across an entire layer of content service providers.

The fact that organisations providing content services, such as Facebook, Twitter and Google are based outside of Australia also warrants close consideration in relation to how obligations in the Act can be imposed on them. The Associations strongly believe that obligations should not be imposed on Australian based service providers that put them at a disadvantage compared to similar service providers located outside of Australia. The Associations note that improved outcomes for LENSAs are expected from improvements to the mutual assistance programs of respective host countries for these various content services.

Recommendation 15

The Associations note that the processes associated with the current exemption regime are overly bureaucratic and are a good candidate for review with the objective of reducing red-tape and unnecessary costs.

For example:

- Resale – currently an annual exemption request must be made for all resold services. Even though it is practically impossible for a reseller to put in place an interception capability as a reseller has no network or facilities upon which to base an interception capability.
- Trial exemptions – in practice, the required date for a commercially practicable trial goes past before a response from the ACMA is received, and even then, the conditions associated with the "exemption" are that a "nominal interception capability" is provided. This is despite the fact that no such concept for a "nominal interception capability" is included in the legislation and that, by its very nature, it would obviate the need for an exemption.
- Some specialist communication services, such as those supplied to corporate and government users, are very unlikely to be intercepted by LENSAs and the provision of interception capabilities is impractical or extremely costly. Nevertheless, every year service providers must go through the bureaucracy of requesting exemptions for these types of services. A simpler, effective approach would be to establish an across the board exemption to all providers of such services, for example, services such as ESCON and FICON.

The Associations suggest that clear criteria should be established regarding the factors that can be used in the evaluation of exemption requests. The granting of exemptions should be based on a reasoned estimation of the risk to LENSA operations balanced against the utility of the service to the community and the interests of carriers and service providers. While LENSA views are clearly important in the evaluation process, the outcome should not be determined solely on that basis.

Recommendation 16

The Associations strongly maintain that carriers and/or CSPs should not be required to decrypt communications that are encrypted by the end user.

Recommendation 17

The industry supports the automation of routine data requests by LENSAs. As LENSAs would be the beneficiaries of automation, the associated costs of automation should be recoverable from the LENSAs. The specification of the time periods for responses should be a matter for each agency to evaluate against the costs they are prepared to pay.

Recommendation 18

The telecommunications industry view is that the overwhelming trend towards IP based communications coupled with the availability of separate "probe" based equipment capable of interception functions provides an opportunity for a complete recasting of responsibilities for interception. Industry obligations should be limited to the supply of an appropriate point for the connection of Agency owned and operated probe based interception capabilities.

The Associations do not support the establishment of obligations based on "tiers". This simply opens up opportunities for criminals to bypass the entire interception regime and to communicate with impunity on lower tiers. It fundamentally undermines the "Tier 1" capital sunk on interception and related functionality.

Recommendations 42

The Associations note the lengthy commentary on the issue of data retention as provided in a submission to the PJCIS Review.

The Associations maintain that any requirement to retain data should not impose any obligation to create or store data that would not be created or stored in the normal course of business. For example, a provider that offers unlimited voice calls does not have a business requirement to record B-party numbers. A data retention requirement that included B-Party numbers would therefore, in effect, impose an obligation on providers to create and retain records on customers solely for the purposes of LENSA surveillance.

Also, for the purposes of data retention, communications data must be clearly distinguished from the content of communications. And where content cannot be separated from data, the information should be treated as content and a warrant must be required for lawful access.

Also, the cost of retaining data beyond any period it would be retained in the normal course of business must be borne by the agencies that require it.

Similarly, any costs in relation to security, storage and ability to search retained data must also be borne by the agencies that require it. The Associations note that keeping more data or keeping data for longer periods, may add to costs significantly whereas the added benefits may be incremental, at best.

The Associations also note that a data retention scheme will involve an increased risk to the privacy of Australians and provide an incentive to hackers and criminals. Data retention is at odds with the prevailing policy to maximise and protect privacy and minimise the data held by organisations. Industry believes it is generally preferable for consumers that telecommunications service providers retain the least amount of data necessary to provision, maintain and bill for services.

The costs of acquiring and retaining particular items of data will vary widely, as will the benefits to LENSAs. An omnibus data retention regime runs the risk of mandating costly retention of data that has limited benefit to LENSAs. Should the Government decide to proceed with a data retention regime, consideration should be given to a legislative framework based on:

- legislative provisions to establish a regime
- subordinate legislation to identify each data element that must be retained, and the specific retention duration for the data element
- a rigorous process to justify the inclusion of any particular data element to the data retention regime, including privacy impact, costs, benefits and community views.

The Associations submit that any data retention regime must contain rigorous controls to prevent the regime from being extended to require carriers/CSPs to collect data that is not required for any

business purpose, as any such action would extend data retention into a Government mandated surveillance regime.

Also, information held in network equipment on a transient basis solely for the purpose of carrying communications must be excluded from any concept of data retention. Any data retention obligations should be confined to data held in IT systems, and specifically exclude any transient data within network elements and exclude data captured for fault investigation and maintenance and repair of network equipment.

The Associations note that any assumption that the identity of the person involved in any communications can be validated is unfounded. This assumption can be readily undermined via identity theft, identity fraud and secondary trading in prepaid mobile services. The assessment of the benefits of any data retention regime must allow a significant discount for ID theft, ID fraud and secondary trading and recognition that organised criminals, terrorists and other persons of interest to LENSAs are more likely to make every attempt to conceal their true identity.

In order to reduce the regulatory burden associated with data retention, any data held specifically for compliance to data retention obligations should be exempt from any customer inquiries under the Privacy Act. The assumption can be that if the legislation requires certain types of data to be retained, then they will be retained.

Recommendation 43

The Associations agree that effectiveness should be demonstrated against specific quantitative criteria.

ALRC Recommendations:

Recommendation 71.2

The Associations agree that clarification of how the various pieces of legislation interact and work together would be most useful for industry.

The Associations suggest that it could provide clarity if requirements and obligations on telecommunication service providers were all contained in the Telecommunications Act and the TIA Act set out requirements and obligations for LENSAs.

The Associations submit that the TIO is not a relevant industry body for the purposes of this Review; however some clarification of the role of the ACMA would be useful.

71.2 (a)

The terms of this point in recommendation 71-2 are quite broad. This submission has focussed on TIA Act and related matters. Other submissions to Government, particularly in relation to the removal of red tape and regulatory burdens more generally, will be made separately from this submission.

Points made above in relation to the PJCIS recommendations 7, 14 and 42 are pertinent to this point.

71.2 (b) and (c)

Please see points made above, in particular points made against PJCIS recommendation 9.

71.2 (d)

One of the objectives of the Telecommunications Act 1997 is to make maximum use of industry self-regulation. However, there is a tendency in relation to matters associated with the Act for Government to formally regulate, predominantly with legislation and to some extent by Ministerial Directions. The Associations suggest that there may be opportunities for greater use of industry codes. For example, industry has proposed in the past that industry codes could be used to define data retention periods for specified data elements, but AGD has opted to pursue changes in primary legislation to introduce a data retention regime.

71.2 (e)

Any public interest monitor should be focussed on the actions of the law enforcement and national security agencies. Additional reporting and oversight obligations for the telecommunications industry are not supported.

Additional Comments

Part 5-4A of the Act

The Part 5-4A process adds additional bureaucracy but the Associations question whether it also adds any value, as requirements already exist in relation to Interception Capability Plans (ICP). Also, directions allowed under Part 5-4A only relate to delivery capability and LENSAs are able to specify delivery capability without relying on Part 5-4A. The Associations believe that Part 5-4A only adds uncertainty and potential delays to the roll-out of new projects and capabilities. The process outlined in Part 5-4A is subject to change at any time, prohibiting business certainty of any outcome.

Delivery Points

The definition of delivery points in the Act is unsatisfactory and does not provide industry with a useful or practical concept. Under the current Act delivery points are defined by Carriers/CSPs but can be subject to dispute. The only guidance provided in the Act as to how delivery points can be defined is: "point from which lawfully intercepted information can most conveniently be transmitted". This is open to disagreement by each LENSA. It also fails to adequately consider national organisations that have a single Delivery Capability. It leaves open the question as to where such a Delivery Capability should be placed, or whether multiple Delivery Capability systems are required to suite the preferences of each individual LENSA for their Delivery Point? Finally the concept, as defined in the Act, fails to recognise the impact of transmission performance between Carriers/CSPs and LENSA monitoring centres; and between Interception Capability and Delivery Capability.

Interception Capability Plan Process

The Associations point out that the obligation to submit an ICP is not applied uniformly across industry members. This potentially allows some CSPs to operate without interception capabilities and provides an avenue for those with criminal intent to bypass interception capabilities.

Section 195(4) of the Act allows for the specification of the content of ICPs but also allows for the extension of obligations on notified CSPs. The Associations submit that any extension of obligations should be made by disallowable instruments to provide full visibility and oversight of any expansions of the interception regime. This power to extend obligations contained in Section 195(4) is yet another source of uncertainty around the scope of industry obligations and requirements under the Act and its regulatory framework.

Conclusion

The Associations welcome further discussion on the Terms of Reference for this review and any questions relating to this submission should be directed to:

Visu Thangavelu
Project Manager, Communications Alliance
v.thangavelu@commsalliance.com.au or 02 9959 9124; or

Lisa Brown
Policy Manager, AMTA
lisa.brown@amta.org.au or 0405 57 00 59.