Communications Alliance/AMTA Submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) – Review of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014.

Submission prepared by:

Communications Alliance Ltd and Australian Mobile Telecommunications Association

12 December 2014

Table of Contents

1. Introduction

Communications Alliance and the Australian Mobile Telecommunications Association (AMTA) – "the Associations" – and their Carriage Service Provider (CSP) members are pleased to have this opportunity to make a submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) review of the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*.

The CSP sector has previously expressed its view, for example in submissions and testimony to the PJCIS in 2013, that it did not believe the Agencies, Attorney-General's Department nor Government had yet made a sustainable case for the imposition of a mandatory data retention regime in Australia. One significant consideration highlighted at that time was the potentially enormous cost impost on CSPs – and therefore, ultimately, Australian consumers. This view has not changed.

This submission has, however, been drafted in constructive spirit – it does not seek to tear down the Government's proposal, but rather to point to a range of areas in which we believe that further consideration is warranted; to clear up areas of ambiguity or internal conflict, avoid unintended consequences, refine or improve processes and implementation and to test the proportionality of what is being proposed. Indeed, we see the PJCIS as a crucial mechanism to test the proportionality of what is proposed in the Bill and the regulations.

As discussed in the body and **Recommendation 1** of this submission, agencies will naturally tend to 'ask for everything' because completeness lowers the risk of any small detail being missed. But when telecommunications users and taxpayers are liable for the cost of 'everything', some discipline should be applied to the scope and volume of agency requests, to increase the likelihood that the national cost incurred is reasonably proportionate to the additional national security garnered.

Industry emphasises that there is a long and productive history of cooperative interaction between service providers and Law Enforcement and National Security Agencies (LENSAs) to meet the general needs and specific requests of agencies in relation to warrantless and warranted information requests and data preservation notices.

These relationships – bolstered by the goodwill of industry in circumstances where interception capabilities are funded by industry – should not be forgotten in terms of the contribution industry has have made over many decades, and continues to make, to Australian law enforcement effectiveness and the enhancement of Australia's national security.

The Government has now introduced legislation to provide for a mandatory data retention regime, within which the Government has undertaken to make a significant, but as yet unspecified, contribution to the capital expenditure requirements that will fall upon the approximately 600 CSPs in Australia.

This industry submission to the PJCIS is made in circumstances where industry:

- cannot yet calculate the financial liability it is being asked to take on (over and above the promised but as yet unspecified Government contribution to required capital expenses) in order to comply with the regime;
- does not yet have clarity on a range of a number of operational requirements, costs and obligations deriving from the regime: and
- remains uncertain whether the scope and operational/financial imposts of the proposed regime are proportional to the security threats facing Australia

Nonetheless, the Associations and their CSP Members have worked in good faith with Departments and Agencies during recent weeks as part of the Industry/Government Data Retention Implementation Working Group, in a bid to clarify the draft dataset proposed by Government and to deal with several related issues.

This submission provides a relatively high-level summary of the key implementation issues that industry foresees if a data retention regime is introduced, along with a series of observations and/or recommendations that industry believes the PJCIS might usefully include in its consideration of the Bill.

Industry would be pleased to offer more detailed material to the Committee during the course of its deliberations and to appear before the Committee if the public hearing schedule allows.

The Associations

Communications Alliance is the primary telecommunications industry body in Australia. Its membership is drawn from a wide cross-section of the communications industry, including carriers, carriage and internet service providers, content providers, 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.

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.

2. Industry engagement on data retention

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.

National security is a concern for all Australians and brings shared responsibilities to the Government and industry alike. However, data retention requirements must be clear, consistent and workable, without imposing unreasonable obligations or unrecoverable costs on industry, or unreasonably impinging on the privacy of our customers.

The Associations have appeared several times before this Committee and have made submissions to this Committee and to other consultation processes regarding various Government proposals for a mandatory data retention regime as follows:

- Feb 2014 – The Associations made a joint submission to the PJCIS on the Terms of Reference for the *Inquiry into a Comprehensive Review of the Telecommunications (Interception and Access) Act 1979*

- August 2012 – The Associations made a joint submission, responding to the PJCIS Inquiry into *Potential Reforms of National Security Legislation – Equipping Australian against emerging and evolving threats.*

- Apr 2010 – Industry response provided to AGD 'Carrier-Carriage Service Provider Data Set' paper

- Oct 2009 - Industry response provided to AGD's Consultation Papers on the Carrier-Carriage Service Provider Data Set, and the Storage Model, in a potential mandatory data retention regime

- Feb 2009 - Industry Position paper on data retention was distributed to Senator Conroy, the Attorney-General's Department, AGO and Department of Broadband, Communications and the Digital Economy (DBCDE)

- March 2008 - Industry views were provided to the Attorney-General's Department on a proposed data retention regime

3. The Dataset & Regulation vs Legislation:

As noted in Section 1 of this submission, Communications Alliance and its CSP members participated in the Industry/Government Working group that was established following the introduction of the Bill, in order to, among other things:

> refine the draft dataset and, specifically, the draft text of regulations to capture the dataset retention requirements; and
>
> look at services that might be suitable for exemption from the regime (refer Section 6 of this submission).

Numerous industry representatives also worked on a 'technical-experts' group that was established to provide advice to the main working group.

All members of the working groups participated diligently and in good faith, but the very short timeframes prescribed for the exercise presented challenges to completing the assigned tasks.

After taking account of industry contributions, AGD made additions and amendments to the explanatory notes and examples that accompany the regulation text, and these did act to lend some greater clarity to various aspects of the dataset.

AGD also agreed to make some minor changes to the data set itself, as outlined in the Implementation Working Group report to the Government..

Industry remains concerned, however, about the use of open-ended language such as "any" in the regulation text. The issue is that although AGD is willing to provide verbal reassurance at this stage about the reasonable intent of the language, there is a risk that, down the track and once the Bill is passed, open-ended language can be used by agencies to demand much more of CSPs in order to demonstrate compliance.

Industry believes there are some simple and reasonable compromises available to further improve the clarity of the regulation text. As one example, when the regulations call ***for "Any identifier"***, this could be replaced by words such as ***"at least one identifier sufficient to enable the source or destination of communications to be identified"***. This would seem to meet the desires of agencies without leaving as much room for later re-interpretation.

As a general principle we also support moving as much of the regulation back into legislation, as outlined in the recommendation below.

Industry's stance on this point appears to be supported by the **Senate Standing Committee on the Scrutiny of Bills**, which reported in November this year, after reviewing the Bill, that:

"The explanatory memorandum justifies the delegation of legislative power on the basis that this is necessary to ensure that data retention obligations remain

'sufficiently flexible to adapt to rapid and significant future changes in communications technology'," the committee reported.

"In light of this, the committee does not consider paragraph 187A(1)(a) to be an appropriate delegation of legislative power. As noted by the Parliamentary Joint Committee on Human Rights (PJCHR) … a scheme which requires that data be collected on every customer 'just in case that data is needed for law enforcement purposes is very intrusive of privacy'.

"Given this, it seems appropriate for Parliament (not the executive) to take responsibility for ensuring that the scheme is adequately responsive to technological change in the telecommunications industry."

Recommendation 1: That as much as possible of the dataset be captured in legislation, rather than in regulations, to guard against unforeseen future 'scope-creep' through

- the broadening of the types of data required to be created and/or retained; or
- the broadening of the range of services that are captured by the data retention regime.

Industry recognises that a justifiable case may arise for broadening the dataset and/or the service set, but recommends that there should be some form of cost-benefit analysis or Regulatory Impact Statement made available to Parliament when agencies/Government/CAC seek to expand the scope of the regime via regulation. This would enable an assessment to be made as to whether such proposals are reasonable and proportionate in light of the technical, operational and financial implications for service providers and their customers, compared with the incremental benefit that would flow to the ability of agencies to prevent or counter serious crime and threats to national security. Such an examination would also highlight whether a supplementary Government contribution to the cost of compliance with the regime is warranted.

Recommendation 2: That – in line with the recent indication from the Attorney-General's Department during Working Group discussions - any change to regulations, in particular relating to services within scope of the regime and requested new data points for retention within existing services, should not be able to be made with immediate effect. Rather, any changes should take effect only after the end of the disallowance period uncontested. This requirement should be explicitly stated within the legislation. Industry should be given sufficient time to consider any proposed addition to the dataset, prior to it being prescribed by regulation and, if necessary, prepare a data implementation plan for approval.

4. Proposed Retention Duration

The duration for which data is required to be maintained by service providers under the regime has wide-ranging implications, including but not limited to:

- the cost to service providers (and Government) of the regime;
- the extent to which individuals' right to privacy is compromised; and
- the attractiveness of retained data to civil litigants of many descriptions and to criminal elements that might seek to access the data for malevolent purposes, such as identity theft.

Industry believes that relevant data should be retained for the shortest duration necessary to support the operational requirements of agencies and that irrelevant data should not be retained at all, unless it is needed for commercial or customer service purposes.

We note that:

- the Parliamentary Joint Committee on Human Rights in November 2014 recommended that the proposed two-year retention period be re-examined, in light of the fact that very few agency requests relate to data more than 6 months old;
- Section 187K(1)(c) of the Bill provides the ability for the Communications Access Coordinator to vary, in relation to a specified service provider (or all service providers) the retention period specified in Section 187C to apply to a specified kind of relevant service.

Industry notes that an appropriately defined data set relating to the standard telephone service and a requirement to retain such for a period of two years, as requested by agencies and proposed by Government, would be close to current industry practice.

Industry is, however, far from convinced that a two year retention period for IP-related data is either necessary, justifiable, cost-effective, or in the public interest. That said, there is some debate among our members as to whether the potential greater simplicity of having a uniform retention period for all services is outweighed by the expense of and complexities of building to a longer than necessary retention period for non-telephone data.

Attachment 1 provides a snapshot of how EU countries have dealt with the question of duration periods. Retention periods typically are between 6 months and 12 months. For internet-related data there is only one country – Poland – that appears to be heading down the path of a 2 year retention period – and that regime is under challenge.

We know that in UK, for example, over a recent 4 year period, 74%+ of disclosures to law enforcement agencies, where the age of data being sought was known, related to data that was less than 3 months old.

We are yet to hear from Australian security agencies a substantive justification for a two year retention period for this category of data, but we would welcome the

opportunity to receive such a briefing and to discuss the practical and operational implications of various duration options.

CSPs report that the vast majority of warrantless requests they receive from Australian agencies relate to data that is 6 months old or younger. It might be useful to incorporate within the Bill a requirement for agencies to periodically report to Parliament the number of requests (including distinguishing between a request relating to an individual and requests relating to groups of people) that have been placed with CSPs for retained data that was generated in the preceding 3 month period, 3-6 month period, 6-12 month period, 12-18 month period and 18-24 month period.

Recommendation 3: A majority of the Associations' CSP members that have contributed to this response believe that a period in the order of 6 months would be an appropriate minimum time to require the retention of internet-related data as part of an Australian data retention regime. We note that it would be entirely feasible to commence a regime on this basis and to examine as part of the PJCIS three-year (or earlier) review of the legislation whether this retention period is optimal, or in need of modification. Consideration should also be given to a requirement for agencies to report annually to Parliament on the 'age-distribution' of the data that they request from CSPs and the relative utility of differing age-category data.

Recommendation 4: We further recommend that CSPs have the flexibility to retain internet-related data for up to two years if they choose to do so, in line with the desire of some services, as, explained above, to standardise their internal requirements. To enable this, the legislation should contain a provision to make it clear that such data can be retained for up to two years without exposing the CSP to a potential breach of the Privacy Act requirement that personal information be kept for no longer than it is required to be retained.

5. Definitional Issues

The Bill, as currently draft carries some definitional challenges for CSPs that would be seeking to ensure compliance with its requirements

The Attorney-General's Department use of telecommunications-specific terminology is not necessarily consistent with the manner in which the same terms are understood and applied operationally by industry. A common understanding of data set terminology is crucial to ensuring that retained data is both relevant to the needs of Government and negates any need for industry to create new data in order to comply with a differing interpretation.

The term "communications" is not defined in the Bill, but is defined in the *Telecommunications Act 1997* as detailed below:

> **communications includes any communication:**
> a) whether between persons and persons, things and things or persons and things; and
> b) whether in the form of speech, music or other sounds; and
> c) whether in the form of data; and
> d) whether in the form of text; and
> e) whether in the form of visual images (animated or otherwise); and
> f) whether in the form of signals; and
> g) whether in any other form; and
> h) whether in any combination of forms.

This definition carries a much wider scope than appears to be the intent of the Bill.

Further the *Telecommunications (Interception and Access) Act 1979* defines "communication" to be:

> ***communication*** includes a conversation and a message, and any part of a conversation or message, whether:
>
> a) in the form of:
> *i) speech, music or other sounds;*
> *ii) data;*
> *iii) text;*
> *iv) visual images, whether or not animated; or*
> *v) signals; or*
> b) in any other form or in any combination of forms.

Similarly, such a broad definition, if it holds for the amending legislation, will create uncertainty in the minds of service providers seeking to comply.

The Bill also does not define "infrastructure", but this is a key consideration for the intended scope of the legislation and which CSPs are to be subject to it.

The Telecommunications Act 1997, however, does define "facility" as follows:

> ***facility*** means:
> (a) any part of the infrastructure of a telecommunications network; or

(b) any line, equipment, apparatus, tower, mast, antenna, tunnel, duct, hole, pit, pole or other structure or thing used, or for use, in or in connection with a telecommunications network.

The TIA definition of facility defers to the above.

Para 32 of the Explanatory Memorandum to the Bill says:

"The term infrastructure should be given its natural meaning within the context it appears. The intention of paragraph 187A(3)(c) is that Part 5-1A will apply to a service is the person operating the service owns or operates infrastructure in Australia relating to any of its services, irrespective of whether the person owns or operates infrastructure in Australia relating to the particular service in question."

So the meaning of infrastructure should be determined in context, but the context appears to be that the "infrastructure" can relate to "any" of the services offered by the relevant "service provider". This could be retail services, marketing services. etc.

Accordingly "in context" it appears that reference to "infrastructure" should not be read as though it is a reference to a "facility" as defined in the Acts. Infrastructure appears to have a very wide meaning which could be along the lines of the dictionary definition i.e.:

3. *the buildings or permanent installations associated with any organisation, operation, etc* (Macquarie Dictionary)

It is also worth noting, in considering appropriate (and consistent) definitions, that the concept of 'facility' has an extended meaning when used in the context of facilities access (see cl17(5) of Sch. 1 to the *Telecommunications Act 1997*):

(5) A reference in this clause to a facility is a reference to:

a) a facility as defined by section 7; or
*b) **land** on which a facility mentioned in paragraph (a) is located; or*
*c) a **building** or **structure** on land referred to in paragraph (b); or*
d)customer equipment, or customer cabling, connected to a telecommunications network owned or operated by a carrier.

Recommendation 5: That further work be undertaken by the Committee and/or Department to bring greater clarity and consistency to the definitions within the Bill. The Associations and their CSP Members would be pleased to participate in such work.

6. Exemptions

Industry seeks a greater level of up-front certainty in terms of data elements or services which are to be exempted from retention obligations in order to allow for long term IT infrastructure planning and to allow industry to build systems accordingly. We believe that appropriate exemption provisions are crucial to limiting the 'red-tape creation' that will inevitably flow from a data retention regime and to achieving proportionality.

In respect of over the top (OTT) services, industry proposes that it provide Government with examples of the types of OTT services which currently traverse telecommunications networks in order to assess which of these types of services might warrant an up-front exemption. Particular attention is drawn to Layer 2 type services such as IPTV, on-demand movie services and Fetch TV, which are effectively content only, along with other Layer 2 services which are, in essence, private communications that traverse public networks.

Industry opposes any proposal that might place responsibility on a carrier for OTT services that are not offered by the carrier itself.

Further consideration also needs to be given as to how bespoke customer solutions, as typically offered to large corporate customers, might be considered within the context of the exemption framework.

Attachment 2 details a list of services that are, in industry's view, strong candidates for up-front exemption from the regime, along with the reasons why we believe this is so.

It is worth noting that proposed section 187K (7) of the Bill, dealing with matters to be taken into account in relation to considering an exemption, states that the CAC must take into account - *the interests of law enforcement and national security*

A common theme behind the listing of many of the services in Attachment 2 is that in industry's view the interests of law enforcement and national security agencies will be very low to negligible in relation to those particular types of services.

7. Service Providers or Services Not Covered

Section 187B of the Bill seeks to exempt, governments, universities and corporations from the obligation of retaining telecommunications data in relation to their own internal network as per Explanatory Memorandum, paragraph 52, page 47. However, the Explanatory Memorandum also states that "the CAC can declare that data from such services must nevertheless be retained" (paragraph 52 re 187B(1)), and "Subsection 187B(2) will provide that the CAC can declare that the provider of an 'immediate circle' or 'same area' service (as defined in subsection 187B(1)) is nevertheless required to retain telecommunications data in relation to the relevant services according to the requirements of subsection 187A(1)" (paragraph 56 re 187B(2)).

Section 187B(2) of the Bill indicates that such a declaration applies in relation to a relevant service that a "service provider" operates. It is therefore unclear whether the CAC is able to declare a service as being subject to data retention, unless it is operated by a service operator - in which case the Explanatory Memorandum appears to be confusing.

Recommendation 6: That the Committee clarify the ability of the CAC to declare a service operated by a government, university of corporation to be subject to data retention.

8. Oversight & Warrant Arrangements

Oversight: The Bill provides for oversight by the Commonwealth Ombudsman in relation to the range of agencies that are able to access telecommunications data, and in relation to the compliance of agencies with the scheme.

We note that the PJCIS previously recommended (Recommendation 42) that the Inspector-General of Intelligence and Security also be given an oversight role.

> **Recommendation 7:** That the Committee consider whether the proposed oversight arrangements will provide for sufficiently rigorous and real-time monitoring of the data retention regime, to guard against 'scope-creep', over-reach by agencies and the adequate protection of consumer privacy.

Warrants & Access Arrangements: Among the country-specific arrangements described in Attachment 1, a majority of countries require some form of judicial authorisation to enable authorised agencies to access retained data.

It seems somewhat ironic that agencies in Australia require a warrant to seek access to the content of communications, but can make a warrantless request for a large volume of individuals' metadata – a body of data that, sufficiently analysed, can potentially create a much more detailed and telling picture of an individual's life and activities than is likely to be gleaned from the contents of a single message obtained under warrant.

The ACMA annual report, released on October 2014 revealed that there were 563,012 authorisations granted to government agencies for access to telecommunications metadata in the 2013-14 financial year.

Industry noted with interest the comments of the former ASIO Director-General, David Irvine, who was reported in the news media on 8 August 2014 to have said that the agency could accept the introduction of a "generic" warrant process to provide authorisation for metadata requests.

Industry believes that some form of expedited warrant or similar process might prove to be a useful tool to ensure that agencies are less inclined to make excessive numbers of metadata requests, and could do so without unduly hampering agency operations.

> **Recommendation 8:** That the Committee consider the appropriateness of a stronger process for authorising metadata requests that are currently warrantless, including whether a "generic warrant" regime might serve to reduce the volume of the present warrantless requests, without unduly hampering agency operations.

9. Unintended Consequences: Privacy, Personal Information and Litigious Access to Metadata

Individual Access to Metadata: The Bill does not explicitly address the question of whether individuals should have the right under Australian Privacy Principle 12, to make demands upon CSPs to provide access to their personal metadata, especially the metadata captured by the mandatory data retention scheme.

This issue is, however, already being tested through a complaint by a journalist to the Privacy Commissioner, seeking a determination on whether a specific CSP should be required to make that individual's metadata available to him. Such a precedent, if established, would be enormously problematic for CSPs.

The metadata relating to an individual do not sit neatly bundled within the operating systems of CSPs. They are typically spread across multiple systems and much of the metadata are network-generated and unintelligible to any person and to systems other than those specifically designed and programmed to interact with those metadata.

The size and cost of the task for a CSP to pull together and make available all the metadata relating to an individual should not be underestimated. The prospect of potentially millions of Australians making such requests to CSPs is little short of frightening. Such a scenario would generate enormous expense and resource demands on CSPs, for no clear or positive outcome. CSPs would need to create purpose-built security and management systems to meet the additional demands imposed on them by this new requirement.

The Associations stress that we are not advocating any restriction on customer access to the Personal Information stored by CSPs about their customers – data such as billing information, address and identification details. This information should continue to be freely available to customers – as is already provided for by the Privacy Act and the Communications Alliance *Telecommunications Consumer Protections (TCP) Code, 2012,* which is registered by the Australian Communications and Media Authority (ACMA).

Recommendation 9: That the Committee consider how to make explicit that CSPs are not required to provide individuals access on-demand to their retained metadata, while reinforcing that the right to individual access to personal information stored by CSPs should and will be maintained.

Litigious Access to Metadata: There has been understandable public concern expressed that, once it is clear that increased volumes of metadata are being retained by CSPs for a specified period, these data will become a 'honey-pot' for civil litigants, who may seek court orders to obtain access to metadata for use in court proceedings. Such actions could stem from Family Law cases and all manner of commercial disputes.

If such a practice were to become commonplace there are serious financial implications for CSPs. Moreover, such a practice would be manifestly outside the

intended objectives of a data retention regime, and therefore should be guarded against.

Recommendation 10: That the Committee investigate ways to prevent the intent of the data retention regime being abused through the emergence of civil litigants seeking and gaining access to retained metadata.

10. Efficacy

Industry has long contended that any data regime introduced in Australia should be proportional to the security threats facing the nation. That is, the costs and other impositions generated by the regime, and the unarguable erosion of individual privacy that flows from such a regime should be carefully assessed and weighed against the reasonably projected improvements in the ability to deter, prevent and investigate serious criminal activity and threats to national security.

Such an assessment needs to also take account of the threats to the effectiveness of the scheme – particularly the extent to which it will be rendered less effective by the avenues to circumvent it.

A recent search of the Apple Store, for example, revealed no fewer than 267 secure messaging applications on offer – each of which is readily obtainable and potentially able to remove the user from the reach of the proposed data retention regime.

Encryption is already available on some smartphones and can be deployed by consumers in numerous ways to protect their communications from scrutiny. The use of Virtual Private Networks is booming across the globe and in Australia, providing yet another means of avoiding data retention.

More sophisticated means of masking communications are also available and widely used by criminal operatives.

This is not an attempt to argue that a data retention regime could not assist Australian security agencies, but rather that the question of proportionality should be tested before Australia embarks on a regime that will impose costs upon, end erode the privacy of, all Australians.

Recommendation 11: That the Committee consider whether the data retention regime as proposed in the Bill constitutes a proportional response to the criminal and security threats facing Australia.

11. Costs to Australian CSP Sector & Level Playing Field

The Abbott Government has consistently proclaimed its commitment to deregulation and to lifting the regulatory burden from industry, including through its Red Tape Reduction initiative. Significant progress has been made against this objective in many portfolios, including by the Minister for Communications and his Parliamentary Secretary in the Communications portfolio.

In the Attorney-General's portfolio, however, the traffic visible to CSPs has been predominantly in the opposite direction – toward the creation of additional Red Tape, regulation and expense.

We note the relevant element of Recommendation 42 of the PJCIS in its June 2013 report on national security issues that: **"Any draft legislation should include the following features: the costs incurred by providers should be reimbursed by the Government";**

Industry concurs with this PJCIS recommendation.

It is presently unclear to us what the level of contribution the Government will make toward the capital-expense of complying with the proposed data retention regime. Indications from Government to date imply that it will not amount to full reimbursement, but the extent of the reimbursement remains unclear.

The Explanatory Memorandum notes that existing cost-recovery arrangements covering data requests by agencies will apply to the operating expenses incurred by CSPs. The data retention regime adds considerable cost to operationalise the cataloguing, storage, collation searching and delivery of metadata and to add additional security to the retained data.

We believe that cost-recovery should also be explicitly provided for in circumstances where civil litigants are also able to make requests for access to metadata.

We would like it to be noted that anything less than full reimbursement by Government of CSP costs will constitute an impost on Australian CSPs that will not necessarily be shared by offshore-based or local providers of 'over-the-top' (OTT) services in Australia that do not operate eligible infrastructure in Australia.

Industry does not, at the time of making this initial submission, have all the answers as to how this potential competitive disadvantage should best be ameliorated by Government. Industry does, however, wish to raise it as an issue for potential Committee consideration, and to signal that we would be pleased to contribute to any such consideration.

Recommendation 12:

- that the PJCIS reaffirm its recommendation that CSP costs to comply with a data retention regime should be reimbursed by Government;
- that the PJCIS recommend that the Government's plans viz, complete or partial reimbursement of CSP costs be clarified before Parliament is

next asked to debate the Bill;

- that CSPs should have the right to recover costs if civil litigants are able to make requests for retained metadata; and
- that the PJCIS consider the potential competitive disadvantage that would be created by domestic CSPs bearing the costs of a data retention regime in circumstances where offshore or local providers of services in Australia do not bear an equivalent burden.

12. Other Planned Legislation

In introducing the Bill, the Government also signalled its intention to introduce legislation for an initiative known as the ***Telecommunications Sector Security Reform (TSSR).***

Industry has been in discussion with the Attorney-General's Department and agencies on this topic for several years. In simple terms it is an attempt to ensure that the telecommunications infrastructure in Australia is appropriately 'hardened' against external cyber-attack or cyber-espionage.

The most recent iteration of the TSSR proposal discussed with industry would see telecommunications carriers in Australia forced to contribute approximately $2 million per annum (via an increment to Carriers Licence Fees) to pay for the employment of additional staff in agencies, whose job it would be to monitor the efforts of CSPs to improve the resilience of their infrastructure. Such monitoring could extend to scrutiny of procurement contracts and physical facilities.

Given that the TSSR forms part of the overall framework of security measures the Government is contemplating – and that it also is proposed to entail an additional financial burden on telecommunications carriers – industry requests that it be taken into account in any consideration the PJCIS gives to overall cost issues.

Recommendation 13: That the PJCIS take account of the overall proposed financial impost on Carriers/CSPs flowing form the Government's national security/data retention proposals, including the TSSR.

Attachment 1 - Data retention - overseas experience

Country	**Retention Period**	**authorisation required to access "metadata"**	**Status of Telecommunications Data Retention Regime**
Australia	*2 years*	*No judicial oversight.*	*Data retention bill has been introduced into Parliament.*
Austria			Ruled Unconstitutional
Belgium	Between 1 year and 36 months for 'publically available' telephone services. No provision for internet-related data.	Access must be authorised by a magistrate or prosecutor.	Under challenge
Bulgaria	1 year. Data which has been accessed may be retained for a further 6 months on request.	Access only possible on the order of the Chairperson of a Regional Court	Ruled Unconstitutional
Cyprus	6 months	Access must be approved by a prosecutor if he considers it may provide evidence of committing a serious crime. A judge may issue such an order if there is a reasonable suspicion of a serious criminal offence and if the data are likely to be associated with it.	Ruled Unconstitutional
Czech Republic			Ruled Unconstitutional
Denmark	1 year	Access requires judicial authorisation; court orders are granted if application meets strict criteria on suspicion, necessity and proportionality	Session logging ceased 2014
Estonia		Access requires permission of a preliminary investigation judge	in force
Finland	1 year	Subscriber data may be accessed by all competent authorities without judicial authorisation. Other data requires a court order.	Under review after the CJEU judgment in April
Germany	1 year		Ruled Unconstitutional. No mandatory data retention. In the new Telecommunication Act enacted in 2012 the provisions on data retention were simply deleted and not replaced by a new

Country	Retention Period	authorisation required to access "metadata"	Status of Telecommunications Data Retention Regime
			data retention concept.
Greece	1 year	Access requires judicial decision declaring that investigation by other means is impossible or extremely difficult.	Still in force
France	1 year	Police must provide justification for each request for access to retained data and must seek authorisation from person in the Ministry of the Interior designated by the Commission nationale de contrôle des interceptions de sécurité.	In force
Spain	1 year	Access to the data by the competent national authorities requires prior judicial authorisation.	In force
Hungary	6 months for unsuccessful calls and 1 year for all other data	Police and the National Tax and Customs Office require prosecutor's authorisation. Prosecutor and national security agencies may access such data without a court order	Further constitutional challenge is being prepared as of April 2014
Italy	2 years for fixed telephony and mobile telephony data, 1 year for internet access, internet email and internet telephony data	Access requires 'reasoned order' issued by the public prosecutor.	In force
Lithuania	6 months	Authorised public authorities must request retained data in writing. For access for pre-trial investigations a judicial warrant is necessary	In force
Latvia	18 months	Authorised officers, public prosecutor's office and courts are required to assess 'adequacy and relevance' of request, to record the request and ensure protection of data obtained.	In force
Luxembourg	6 months	Access requires judicial authorisation.	Under review. Luxembourgish Justice Minister on the day of the CJEU judgment announced that a

Country	Retention Period	authorisation required to access "metadata"	Status of Telecommunications Data Retention Regime
			detailed analysis of possible consequences for the national law will be undertaken.
Malta	1 year for fixed, mobile and internet telephony data, 6 months for internet access and internet email data	Requests must be in writing - Malta Police Force; Security Service	In force
Netherlands	1 year	Access must be by order of a prosecutor or an investigating judge	Following CJEU judgment it was reported that various parties in parliament have already stated that the data retention provisions should be abolished completely or in part, and further challenges seem likely.
Romania	(6 months under the earlier annulled transposing law)		Ruled Unconstitutional (twice)
Poland	**2 years**	Requests must be in writing and in case of police, border guards, tax inspectors, authorised by the senior official in the organisation.	Under challenge
Portugal	1 year	Transmission of data requires judicial authorisation on grounds that access is crucial to uncover the truth or that evidence would be, in any other manner, impossible or very difficult to obtain. The judicial authorisation is subject to necessity and proportional requirements.	in force
Slovenia	8 months for internet related and 14 months for telephony related data	Access requires judicial authorisation.	Ruled Unconstitutional. Ordered that data collected under the data retention law be deleted
Slovakia	12 months, 6 months for Internet services	Requests must be in writing.	Ceased following judgment of European Court of Justice. Records deleted.
Sweden	6 months		Under Challenge by ISP Up to 2013 CJEU challenged Swedish govt for their delay in implementing the Directive due to

Country	Retention Period	authorisation required to access "metadata"	Status of Telecommunications Data Retention Regime
			domestic controversy
UK	1 year	Access permitted, subject to authorisation by a 'designated person' and necessity and proportionality test, in specific cases and in circumstances in which disclosure of the data is permitted or required by law.	DRIP - Under Challenge
Ireland	2 years for fixed telephony and mobile telephony data, 1 year for internet access, internet email and internet telephony data	No. Requests to be in writing.	Under Challenge
Switzerland[i]			Under Challenge
Norway	N/A	N/A	No mandatory data retention regime

11 Member States require judicial authorisation for each request for access to retained data.

In 3 Member States judicial authorisation is required in most cases.

4 other Member States require authorisation from a senior authority but not a judge.

In 2 Member States, the only condition appears to be that the request is made writing.

Since in April 2014 the Directive has been declared invalid from the outset, the EU member states are no longer required to transpose it into their national laws. The member states nevertheless may introduce laws on data retention on a national level, provided those are in line with the relevant constitutional requirements.

Laws on data retention already existing in the member states remain valid as well (save for possible constitutional challenges they are or might be facing on a national level).

Rreferences

[1] Successful first step in challenging Swiss Data Retention, 2 July 2014, available at: http://sustainability.oriented.systems/challenging-swiss-data-retention/

http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/data-retention/index_en.htm

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-05-30_Evaluation_Report_DRD_EN.pdf

http://wiki.vorratsdatenspeicherung.de/Resources

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:en:PDF

http://eulawanalysis.blogspot.com.au/2014/04/national-legal-challenges-to-data.html

http://www.digitalrights.ie/data-retention-slovenia-unconstitutional/

http://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf

http://www.helsinkitimes.fi/finland/finland-news/domestic/10120-finland-must-revise-its-data-protection-laws.html

Attachment 2 - Examples of Services to be Exempt from Data Retention regime

A Services supplied where end user is not identifiable at the Carrier/CSP level and customer base is unlikely to be of interest for national security or serious crime investigations.

Service Name	Type of service	Configuration	Target customers	Reason
MetroWave	Data traffic between data centres	Point to Point	Major Corporate and Government.	End user information not available No source identifiers available to the carrier/CSP No destination identifiers available to the carrier/CSP Time and dates of communications unknown to the carrier/CSP Type of communication unknown to the carrier/CSP Additional compliance costs with no benefit beyond existing record keeping
Virtual Private Local Access Network Service	Data Traffic between customer sites	Point to point or Multi – point.	Major Corporate and Government.	End user information not available CSP routes packets on the basis of the VPN identifier Origin and destination IP addresses ?? Time and dates of communications unknown to the carrier/CSP Type of communication unknown to the carrier/CSP Additional compliance costs with no benefit beyond existing record keeping
Ethernet over Copper (EoC)	An access network that uses bonded copper pairs to provide maximum speeds of up to 22Mbps, depending on the distances from the customer site to the nearest Exchange	Point to point or Multi – point	Major Corporate and Government	
10 GbE Point-to Point	10 Gigabit per second Ethernet over fibre point to point service typically used for connection between data centres	Point to point	Major Corporate and Government	No source identifiers available to the carrier/CSP No destination identifiers available to the carrier/CSP Time and dates of communications unknown to the carrier/CSP Type of communication unknown to the carrier/CSP Additional compliance costs with no benefit beyond existing record keeping
Internet (access) Service	Provides access to the internet using Tier1 providers	Access to internet by corporate and Government customers	Major Corporate and Government	Session information not available. End user information not available. Time, duration and date of communications not available. Ongoing compliance costs for no benefit. Additional compliance costs with no benefit beyond existing record keeping

B Services used for machine to machine communications

Service Name	Type of service	Configuration	Target customers	Reasons
Extranet solution (e.g. Optus brand: EFinity)	Provides an IP based infrastructure to support the evolving electronic commerce and information interchange requirements of financial & business services using the OPI platform.	Available on access links and at storage points.	Major Corporate and Government.	Session information not available. End user detail not available. Time, duration and date of communications not available. Not expected to be utilised by persons of interest to LENSAs. Additional compliance costs with no benefit beyond existing record keeping
Machine to Machine (USIM-based)	Carriage and service management solution that allows customers to communicate with and manage devices in the field. Common applications that utlise a machine to machine solution are: metering, vehicle telematics, environmental sensors, vending machine monitoring and security monitoring	Point to point or Point to Multi-point	Corporate and Government.	Session information not available. End user detail not available. Time, duration and date of communications not available. Not expected to be utilised by persons of interest to LENSAs. Additional compliance costs with no benefit beyond existing record keeping

C Broadcast/Content services

Service Name	Type of service	Configuration	Target customers	Reasons
Satellite Broadcast Services	Includes, Audiocast Home Cast; Multi cast RemoteCast, OmniCast Video Connect (TV link), Aurora solutions.	Available by direct reception of signal..	Major Corporate and Government, Business, Consumer.	Potential high volume data and associated storage costs Broadcast for closed user groups, not necessarily covered by Broadcasting Services Act Broadcast similar to pay tv, but may not be covered by Broadcasting Services Act Content posted by reputable organisations of no interest to LENSAs. Additional compliance costs with no benefit beyond existing record keeping.
On demand movie service	On demand movie service	Point to point service	Consumers	On demand, point to point service not covered by the definition of 'broadcasting service' as contained in s. 187A(3). Content posted by reputable organisations of no interest to LENSAs. Additional compliance costs with no benefit beyond existing record keeping.