Telecommunications and Other Legislation Amendment Bill 2016

Questions on Notice for Industry Associations

Subsequent to Public Hearing on 16 February 2017

Question on Notice agreed at hearing:

1. Industry associations note that the Bill applies only to a subset of the Australian telecommunications sector (i.e. it applies to C/CSPs and intermediaries, but not to over-the-top service providers). Industry suggests the Bill 'fails to adequately recognise the evolution that is occurring in the supply of services over the internet', and that an Australian based C/CSP 'simply re-selling over-the-top services' will face substantial regulatory uncertainty and regulatory risk under the framework. Industry further suggests that a C/CSP should only need to take action under the proposed legislation if the supply by the Australian C/CSP adds a substantial security risk (p15, para 3.8).

    - As discussed at the public hearing, please develop a proposal outlining any additional amendments you seek to the Bill, Explanatory Memorandum and/or Administrative Guidelines?

INDUSTRY RESPONSE:

As per our submission, Industry believes that a C/CSP should only be required to take action under the legislation if the supply of the over-the-top (OTT, e.g. Skype, WhatsApp, Facetime) service by the Australian C/CSP adds substantive security risk. The obligations of C/CSPs should be assessed solely on the basis of the application of the following iterative analysis:

- the level of security risk that applies if the service is obtained directly from the service supplier;
- the level of security risk that applies if the service is obtained via the C/CSP; and
- the steps that can be implemented by the C/CSP to address any <u>added</u> security risk.

This approach could be incorporated into the legislation in two ways:

- By amending s314A(1), e.g. by adding. "…and, where the change relates to the resale of an OTT service from a non-Australian provider through an Australian carrier or carriage service provider, the resale of that service through the Australian carrier or carriage service provider substantially increases the likelihood or potential severity of a materially adverse effect (on the ability of the carrier or carriage service provider to comply with its obligations under subsection 313(1A) or (2A)) already inherent in the OTT service as provided and available to the Australian public from the non-Australian provider."; or
- By adding a 'class exemption' (creating a new s314A(4)) to the law, e.g. "Section 314 does not apply to changes…[and then something along the lines of the above]."

Note that the above would require the insertion of a definition of OTT services in s7 of the Act.

Security Obligation

2. Industry associations are concerned that C/CSPs and intermediaries will be subject to an obligation to protect networks and facilities owned, operated and <u>used by</u> the C/CSP from unauthorised access and interference. Industry has indicated concern

about what the term 'use' may entail and what would be required of C/CSPs and intermediaries to protect networks they are 'merely using'. Industry has sought clarification about the sorts of measures that could be put in place to demonstrate compliance with this obligation (p13, para 3.3):

- Can you please explain your concerns about the term 'used by' and why you consider it to be difficult to demonstrate compliance against this aspect of the security obligation (section 313)?

INDUSTRY RESPONSE:

It should be noted that a CSP has the relationship with an end customer while carriers own and operate the network infrastructure required to enable a communication to be carried. A CSP may also be a carrier, however, in many cases they may neither own nor operate network infrastructure to support the delivery of a communication, as that is the role of carriers.

CSPs can have many arrangements to deliver communications for their customers. These may be via a network that they own or operate under an Australian carrier licence, or they may contract with one or more carriers who may be Australian or non-Australian entities.

Where a CSP is also a carrier, they may also use carrier infrastructure owned and operated by another carrier to deliver a communication within Australia (e.g. national roaming) and they may, or may not, own infrastructure for any international component of a communication. Carriers may own and operate infrastructure within Australia, or they may use local bearers to deliver communications to a non-Australian location where routing is managed.

The obligation of s313 goes to the protection of networks and facilities (refer to the Industry Response at question 4 regarding a discussion on the term facilities) that they own, operate or use. C/CSPs accept an obligation to do their best to protect networks that they own or operate and, consequently, the obligation to maintain competent supervision of and effective control over those networks makes sense. However, it is impossible for C/CSPs to directly protect networks that they use but do not own or operate (say under a wholesale arrangement with another carrier), precisely because they cannot exercise competent supervision of and effective control over those networks. Where the networks they use are located in Australia, network operators already have obligations of their own under TSSR, so it is not necessary to extend the obligation to wholesale customers of network operators who have no control over the infrastructure.

The transmission of all forms of communications in a very large number of cases implies the use of networks that providers have no direct control over, do not own, manage or operate.

Note that on its way to its destination, voice and data communications will make use of 'least-cost routing' arrangements that are used globally – for example, the voice bearer traffic of a call may be passing through a number of Australian and/or non-Australian networks. The voice signalling traffic required to connect and disconnect the call may yet again use other Australian and/or non-Australian network parts. In addition, the call routing, i.e. which networks are being used, may be dynamic and/or automated and change from hour to hour or even more frequently. Once a call leaves a network used by a CSP or a

network that a CSP operates, that CSP is unable to protect the networks that are being used in the course of this communication.

Consider the following examples:

1. A communication is originated in Australia by a customer of CSP A on an Australian network used by CSP A (who may, or may not, own or operate that network) and routing is carried out dynamically in one or many non-Australian locations and then routed back into Australia on one or more other Australian networks, that may, or may not be, owned or operated by CSP A.
   In this example, other Australian entities may have the obligation to protect their network assets within Australia, effectively meeting the aims of the legislation. The non-Australian portion cannot be 'protected' by CSP A as they may have no control of those networks and may have no control of the routing used by the carriers bearing that communication to its destination.

2. A communication is originated in Australia by a customer of CSP A using an OTT service that may, or may not be, provided by CSP A. The OTT communication is then terminated in the US on US CSP B's network.
   In this example, CSP A may be a non-Australian entity who uses local bearers to deliver OTT services to Australians. The local carrier infrastructure owners may have the obligation to protect their network assets within Australia, effectively meeting the aims of the legislation. Again, the non-Australian portion cannot be 'protected' by CSP A as they may have no control of the networks used by the carriers bearing that communication to its destination.

3. An end user in Australia is using the internet, say to order clothes from an online store (i.e. Amazon) in Australia where the traffic routinely exits Australia to carry out routing activity and then is directed back to Australia.
   In this example, the online store's CSP providing the internet service may be a non-Australian entity who uses local bearers to deliver OTT services to Australians, or a local CSP. In either case the local carrier infrastructure owners may have the obligation to protect their network assets within Australia, effectively meeting the aims of the legislation. As in the other examples, the non-Australian portion cannot be 'protected' by local CSPs as they may have no control of any of the networks components used by the non-Australian carriers bearing that communication to its destination.

It is unclear to Industry how C/CSPs would be able to comply with their duty to do their best to protect networks that they use, given the unavoidable inability to supervise or control those networks.

The lack of clarity in the Bill raises questions in relation to this issue. For example:

Is the Bill envisaging that C/CSPs contractually require owners of all networks that a communication may use to, in turn, do their best to protect those networks? It is important to understand that such networks may be used dynamically, on an automated basis and without prior knowledge of the C/CSP on whose network the communications originated and/or without the knowledge of the C/CSPs whose networks are being used. Consequently, Industry notes that an assumption that contractual arrangements could be used to ensure

protection of networks that are being used ignores commercial and technical realities. CSPs in other jurisdictions may also not allow their national C/CSP to enter into such arrangements.

Alternatively, does the Bill envisage alternative means that would allow Australian C/CSPs to demonstrate compliance with their duty to do their best to protect networks that they use but do not own or operate? If so, Industry would be keen to understand what those means would be, how they are supposed to operate and how C/CSPs could provide proof that their compliance duty has been met.

Industry requests that the legislation should only apply to networks and facilities owned or operated under an Australian carrier licence as the ability to protect networks and facilities resides with the owner operator of that network.

3. Industry associations have raised concerns about 'acts of foreign intelligence services' in the context of whether the reforms would prevent the use of offshoring facilities and sourcing of services from non-Australian. Industry has asked whether having 'an ability to log, within Australia, any lawful access requests made to Australian systems offshore would be sufficient to fulfil the requirement of protecting networks against acts of foreign intelligence services' (pages 13 and 14, para 3.4):

    - Would your concerns about the application of the Bill to infrastructure located offshore be addressed through amendments to the Explanatory Memorandum and Administrative Guidelines to clarify whether C/CSPs would be in breach of the security obligation (section 313) if they acted in accordance with an applicable law of a foreign country?

INDUSTRY RESPONSE:

Yes. Clarification in the Explanatory Memorandum and Administrative Guidelines on the issue of outsourced or offshore arrangements will be vital for industry.

4. Industry associations suggest the term 'facilities' should be clarified. This is particularly because industry are unclear about the application of the Bill to cloud computing and particularly whether cloud computing would be captured under the definition of 'facility' in the Telecommunications Act (p16 and 17, para 3.9):

    - Would industry be satisfied if further clarifying information about the application of the Bill to cloud computing was set out in the Explanatory Memorandum and Administrative Guidelines?

INDUSTRY RESPONSE:

Yes, this would help clarify the situation around cloud computing and its variations.

Further clarification is required to the term 'facility' to exclude those facilities owned or used by a C/CSP that are not used to supply carriage services (for example, a facility used to provide content services). In the interest of certainty, this aspect may be best dealt with via the definitions in the legislation.

Notification Requirement

5. Industry associations are concerned about the existing non-exhaustive list of notifiable items outlined in the Bill subsection 314A(2)). Industry seeks that an exhaustive list of notifiable equipment be incorporated into the Bill. This is because the existing terminology implies that 'just about anything' in the course of normal network and system management must be notified. Industry says this is problematic because it is unclear what measures might be regarded as sufficient protections to meet the obligations (p14, para 3.5):

    - Can you please specify the exact level of detail you would like to see included in the list of notifiable items in subsection 314A (2)?

    - Could this be addressed through amendments to the Explanatory Memorandum and Administrative Guidelines?

INDUSTRY RESPONSE:

Industry suggests that a more specific definition of the changes that, subject to the already included test of material adversity, must be notified ought to be added into the legislation.

For example, the New Zealand *Telecommunications (Interception Capability and Security) Act 2013* (TICSA) stipulates that the changes that are to be notified are limited to "areas of specified security interest" (section 48) and the TICSA itself then goes on to list those areas (section 47).

Adding such a list to the material adversity test while also amending the legislation to only apply to networks and facilities owned or operated (but not used) under an Australian carrier licence (see Industry Response at Question 2) would make the legislation more workable, useful and practical to implement.

6. Industry associations seek that an adverse security assessment should be a requirement for the Communications Access Coordinator to provide advice on a notification (in addition to being a requirement of a direction) (p15, para 3.6):

    - Can industry please explain why specifically you consider an adverse security assessment should be required as part of the notification process?

INDUSTRY RESPONSE:

As noted in section 3.6 of our submission, the prerequisite of an adverse security assessment only applies to the directions powers of the Attorney-General but not to the assessment process by the Communications Access Co-ordinator (CAC) and the consultation process that would precede such a direction. Industry feels that there may be an inherent tendency by the CAC 'to play it safe' which may lead to an increased number of findings that a proposed change involves a risk of unauthorised interference with/access to networks that would be "prejudicial to security". (Note that the latter term is also only described in the Explanatory Memorandum instead of the legislation itself.) The lack of a formal requirement for the assessment of proposed changes allows the CAC to (intentionally or unintentionally)

apply pressure onto C/CSPs. Consequently, Industry seeks a more formal basis for the assessment of proposed changes.

International approaches

7. Industry has raised a number of concerns regarding the approach outlined in the Bill when compared to international approaches (Industry Associations p7, para 2.2). Industry Associations have noted in their submission that the telecommunications security framework adopted by New Zealand caused some companies to relocate their business operations off-shore to countries where the legislative requirements were less onerous:

    - Do you know which aspects of the New Zealand legislation, specifically, might have resulted in these companies deciding to move their business operations offshore?

INDUSTRY RESPONSE:

In 2015, the United States vendor Corse Technology, Google's research deployment at Victoria University of Wellington, the US government Energy Sciences Network in Berkley (CA), and REANNZ (a research network provider) moved a leading-edge SDN (Software Defined Network) testbed project out of New Zealand because the New Zealand *Telecommunications (Interception Capability and Security) Act 2013* (TICSA) and associated guidance material created a degree of uncertainty regarding which forms of network changes (e.g. including second-by-second network changes as they are common in an SDN world) would be covered under the TICSA.

Victoria University of Wellington noted that the testbed operators had sought clarification from the Government Communications Security Bureau (GCSB) but had not received meaningful guidance. Importantly, even though the GCSB noted that it had not requested notification to or authorisation from the GCSB for the changes in question, the uncertainty around the requirements was sufficient to move the project out of New Zealand.

This is even more alarming if viewed in an Australian TSSR context: it appears that the New Zealand TICSA is already significantly more specific regarding the changes that are to be notified than what is being set out in proposed TSSR legislation, i.e. the changes themselves are more clearly defined (Section 48 of the TICSA) and are limited to "areas of specified security interest" with those areas being listed in the legislation itself (Section 47 of the TICSA).

Australian participation in the development of 5G standards and network designs will depend on the C/CSP's ability to access SDN and NFV (Network Function Virtualisation) technologies locally. If similar restrictions are introduced under TSSR that prevent (including through the imposition of unacceptable risk to commercial entities) Australian C/CSPs from participating in the hands-on development of 5G network topologies and standards that are based on SDN and NFV, Australia will fall behind very quickly in the adoption of 5G technologies and will again be subject to the acceptance of non-Australian technology developments rather than having a seat at the table in its development.