House Standing Committee on Infrastructure and Communications Consultation:

Disrupting access to illegal online services using the Telecommunications Act 1997

Submission as prepared by:

Communications Alliance and the Australian Mobile Telecommunications Association

22 August 2014

Executive Summary

Communications Alliance and the Australian Mobile Telecommunications Association (the Associations) welcome the opportunity to comment on the House Standing Committee (the Committee) on Infrastructure and Communications' consultation on Disrupting Access to Illegal Online Activities using the Telecommunications Act 1997 (the Act).

The Associations acknowledge that Sub-section 313(3) (s.313(3)) of the Act establishes a framework that provides law enforcement and national security agencies with an ability to seek assistance from telecommunications service providers. This framework has the flexibility to go beyond circumstances specifically defined in legislation.

The Associations recognise that there are concerns that the broad terms of s.313(3) appears to allow utilisation by non-critical stakeholders. The Associations note that the concept of 'help as is reasonably necessary' has been extended to include the blocking of websites where it is deemed that illegal activity is connected to that site. Use of s.313(3) for this purpose should be restricted to Government enforcement and national security agencies and requires guidelines, safeguards, reporting and established levels of authority from the requesting Agency to ensure that any blocking and the consequences of such blocking has been considered at a senior level, is properly targeted and that legitimate websites and users are not also inadvertently blocked. Further, it is important that there is a quick and efficient review mechanism should someone believe a website has been blocked in error.

1. Introduction

The Associations

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

1.2 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. REQUESTING AGENCIES and SIGN-OFF AUTHORITY

- The Committee has stated in its terms of reference that it seeks to establish a more formal framework for agencies that may make requests under s.313(3). The Associations support a review of the agencies and organisations that utilise the subsection.

- Protecting the privacy of customers is a critical consideration for service providers. Accordingly, the provision of access to telecommunications data under s.313(3) needs to be proportionate and take due account of customer expectations that service providers will protect their personal communications and related information.

- The Associations note that some service providers have received s.313(3) requests in the past from organisations such as the RSPCA and ASIC, and indeed even from non-Government entities such as legal assistance organisations. Clarification is sought from the Committee on how the use of the subsection by non-enforcement agencies should be balanced against customer expectations of privacy.

- The Associations expect that access to telecommunications data under s.313(3) by private citizens is not envisaged. This should be clearly stated in s.313(3).

- In addition to clarifying who is able to use s.313(3), the Associations recommend that any use of s.313(3) should be subject to guidelines or regulations that set out processes and procedures to be used. These should specify, for example, the required level of seniority and minimum technical competence that individuals within an organisation should possess to enable them to authorise a request under s.313(3).

- The Associations note that:

    - the authorisation process under Section 315 of the Act is clearly defined where there is a need to suspend telecommunications services in the event of an emergency; and

    - comments about s.313(3) apply equally to s.313(4) and that s.313(4) should be amended in the same terms as any amendments to s.313(4).

3. Scope of Sub-section 313(3)

- Sub-section 313(3) has been used to limit access to websites that contain prohibited material. This is appropriate, for example, to limit access to child sexual exploitation material. The Associations are now concerned, however, that the subsection is being used to disrupt other online services.

- Use of S.313(3) by non-enforcement agencies has resulted in the inappropriate blocking of legitimate websites, apparently due to a lack of understanding of the potential impacts of the requests being made to ISPs. Use of the section should be restricted to enforcement and security agencies. In addition appropriate controls and processes need to be implemented to ensure proper consideration and consistent application of public policy considerations such as considerations relating to the right to privacy and freedom of speech. There should be a clear and efficient review mechanism where members of the public can report legitimate websites that have been blocked in error.

- Requests under s.313(3) should meet proportionality tests. The Associations highlight the Serious Contraventions test that applies under the Telecommunications (Interception and Access) Act 1979. At this time there does not appear to be an obligation on the requesting agency to demonstrate that due diligence has been conducted prior to making the request.

- A process for ensuring the accuracy or scope of a take-down notice or requesting a redirection to another provider also needs to be defined.

- Costs associated with meeting any s.313(3) request should continue to be met by the requesting agency in accordance with section 314.

4. Conclusion

In summary, the Associations consider that a robust and appropriate s313(3) scheme should:

(i) only be used by appropriate Government enforcement (i.e. organisations dealing with law enforcement at major crime level, national security, and revenue matters of major significance) and national security agencies;

(ii) require due diligence from the requesting agency as to the impact of the blocking on other websites linked to that domain name/IP address;

(iii) require sign-off by a senior officer of the agency;

(iv) require a redirection/landing page that includes the contact details of the agency making the request with legal protection for the provider against the wrongful delivery of communications offence under the Criminal Code;

(v) provide for an appeals mechanism for people to report websites that have been blocked in error; and

(vi) be subject to full cost recovery.

The Associations look forward to continued engagement with the Committee and the Government on the proposed review of Sub-section 313(3) and would welcome the opportunity to discuss, in greater detail, the feedback provided in this submission.

For any questions relating to this submission please contact Visu Thangavelu on 02 9959 9124 or at v.thangavelu@commsalliance.com.au or Lisa Brown on 02 6239 6555 or at lisa.brown@amta.org.au