



House Standing Committee on Infrastructure and Communications

Inquiry into the use of subsection 313(3) of the *Telecommunications Act 1997* by government agencies to disrupt access to illegal online services

Supplementary Submission

**Communications Alliance
and
Australian Mobile Telecommunications Association**

13 March 2015

INTRODUCTION

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>.

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>.

The Associations thank the House Standing Committee on Infrastructure and Communications for having been given the opportunity to appear before the Committee.

This document supplements the submission that the Associations provided in August 2014 to the Committee titled "Disrupting access to illegal online services using the *Telecommunications Act 1997*". This supplementary submission also provides an indication of the kind of requests that providers currently receive and/or are likely to receive in the future under s313(3).

SUPPLEMENTARY SUBMISSION

The Associations propose that Government adds a new section to the *Telecommunications Act 1997* (Act) dealing specifically with the blocking of websites (see further below), while leaving s313 unchanged as it establishes a broad framework for the supply of assistance to officers and authorities of the Commonwealth and of the States and Territories, and in particular to law enforcement and national security agencies. In addition, s313 provides a mechanism by which providers can give assistance to officers and authorities where that assistance is essential, and where that assistance does not fall within the specific provisions of the *Telecommunications (Interception and Access) Act 1979* (TIA Act) or other provisions in the Act and where the assistance does not involve the disclosure of information or communications.

Industry members note that s313(3) covers a range of matters where assistance may be provided, including those specifically mentioned at s313(7) as well as other matters some examples of which are:

1. Modifying provider networks and standing up a temporary line for a hostage situation where the existing line has been suspended under s315;
2. Providing infrastructure support (e.g. mobile cellular devices) enabling mobile telecommunications connectivity for crisis management-type criminal investigations and/or national security impacting events; and
3. Traffic management assistance where an institution is experiencing a large scale denial of service attack which is impacting the wider economy and the delivery of emergency service communications.

Importantly, s313 provides flexibility via subsection 313(3) in that the type of assistance required may emerge well in advance of the ability for Government to place specific obligations into legislation. The denial of service attack is a good example of the type of incidents that emerge from internet technologies, and demonstrates how difficult it is for legislation to anticipate the issues that may arise as technologies and services evolve.

The Associations note that, in their view, s313 should not authorise the disclosure of metadata. It would provide greater certainty if the legislation were to state those matters that are specifically covered by the TIA Act and which must follow TIA procedures in all instances. The Associations contend that the range of agencies making use of s313 (or a similar provision) ought to be more limited than is currently the case.

In addition, the Associations support a form of 'gating process' as proposed by the Department (recommendation 2) in relation to the new section dealing with website blocking. Industry considers that the approval of an agency that wishes to request blocking of websites under the new provision of the Act ought to rest with the portfolio Minister rather than the agency head (permitted agencies), and that sign-off for individual requests rests with a senior officer of the permitted agency.

The Associations propose to add a new section to the Act (similar to the current s315) specifically addressing the requests of disrupting access to online services (blocking websites). The Associations believe that the blocking of websites is more appropriately dealt with within primary legislation rather than a guideline and that the certainty provided through the use of primary legislation constitutes better public policy as it is likely to increase community confidence that the use of blocking websites is proportionate to the potential harm to the community.

The new section ought to (at a minimum):

1. clearly define the circumstances of application of the provision (including a limitation of application to material that draws a maximum prison term of at least two years or financial equivalent);
2. stipulate the process for becoming a permitted agency and the level of seniority of the authorising officer within that permitted agency requesting the blocking of a website;
3. set out the limitations of liability on the part of the service provider (as per s313);
4. require permitted agencies to consult with personnel with the relevant technical expertise within their own agency or agencies that have demonstrated the necessary expertise and competence;
5. require the use of stop pages containing the name of the permitted agency requesting the block, the reason for the block, a point of contact (direct phone number and not just a web link) and a reference as to how to seek review of the decision to block;
6. impose the establishment of a swift review mechanism where website blocking has been appealed; and
7. allow providers to fully recover any costs that they incur as a result of blocking (and unblocking) requests (as per s314).

The Associations note that the proposed new section would not lower the evidentiary barrier or enable corporate entities or individuals to request providers to block a website. It merely seeks to eliminate situations in which providers (via the s313(3) obligation to provide “help as is reasonably necessary”) are obliged to carry out the actions requested by agencies without the agencies being accountable for their requests or the potential consequences.

In addition to the above, the Associations support the development of a permitted agency guideline to address the following issues:

1. The approval of an agency that wishes to request blocking of websites under the new section of the Act to rest with the portfolio Minister;
2. Agencies to develop clear internal policies outlining their processes for requesting blocking of websites;
3. Agencies may also consult Industry and non-Industry stakeholders prior to making a request to block a website but provisions similar to s315(3A) and (3B) will apply under the new section; and
4. All requests for blocking under this new section to be reported to the ACMA (i.e. annual s308 reports) or, where appropriate, to a Parliamentary Committee, and annual evaluation of the requested blocks to ensure the guideline and new section operate within the desired constraints and achieve the desired outcomes.

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

For any questions relating to this submission please contact Christiane Gillespie-Jones on 02 9959 9118 or at c.gillespiejones@commsalliance.com.au or Lisa Brown on 02 6239 6555 or at lisa.brown@amta.org.au.

ATTACHMENT A

For reference only: Copy of s315 Telecommunications Act 1997

315 Suspension of supply of carriage service in an emergency

- (1) If a senior officer of a police force or service has reasonable grounds to believe that:
- (a) an individual has access to a particular carriage service; and
 - (b) the individual has:
 - (i) done an act that has resulted, or is likely to result, in loss of life or in the infliction of serious personal injury; or
 - (ii) made an imminent threat to kill, or seriously injure, another person; or
 - (iii) made an imminent threat to cause serious damage to property; or
 - (iv) made an imminent threat to take the individual's own life; or
 - (v) made an imminent threat to do an act that will, or is likely to, endanger the individual's own life or create a serious threat to the individual's health or safety; and
 - (c) the suspension of the supply of the carriage service is reasonably necessary to:
 - (i) prevent a recurrence of the act mentioned in subparagraph (b)(i); or
 - (ii) prevent or reduce the likelihood of the carrying out of a threat mentioned in subparagraph (b)(ii), (iii), (iv) or (v);

the officer may request a carriage service provider to suspend the supply of the carriage service.

- (2) The carriage service provider may comply with the request.
- (3) This section does not, by implication, limit any other powers that the provider may have to suspend the supply of the carriage service.
- (3A) The provider is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith in compliance with the request.
- (3B) An officer, employee or agent of the provider is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith in connection with an act done or omitted by the provider as mentioned in subsection (3A).
- (4) In this section:

senior officer, in relation to a police force or service, means a commissioned officer of the force or service who holds a rank not lower than the rank of Assistant Commissioner.