5 April 2019

COMMUNICATIONS ALLIANCE LTD
www.commsalliance.com.au

Dr Carolyn Patteson
First Assistant Secretary
Content Division
Department of Communications and the Arts
GPO Box 2154
Canberra ACT 2601

onlinesafety@communications.gov.au

Dear Carolyn,

RE: Online Safety Charter Consultation Paper

Communications Alliance welcomes the opportunity to make a submission to the Department of Communications and the Arts Online Safety Charter Consultation Paper (Consultation Paper).

The communications industry, including internet service providers (ISPs), recognises that access to some online content, particularly by minors or vulnerable adults, may have detrimental effects on the physical, social and emotional well-being of the user and may also influence their values with regards to sexuality, relationships, violence, security, racial and religious equality and tolerance and many other key societal aspects. The proliferation of online social networking poses additional challenges around cyberbullying and the sharing of illegal content.

It goes without saying that illegal content, especially material relating to child exploitation and terrorism, must be removed as quickly as possible, to minimise the detrimental effects on all parties involved.

As in the past, our industry continues to engage closely with all stakeholders, including the Office of the eSafety Commissioner, law enforcement agencies, the Australian Communications and Media Authority (ACMA) and the Australian Competition and Consumer Commission (ACCC), and is keen to assist, where possible, to create and promote a safe online environment.

Purpose and context of the Online Safety Charter

We note that currently there are a number of inquiries and activities underway that go, to a varying extent, to the issues raised in the Consultation Paper. Those include the ACCC Digital Platform Inquiry (DPI), the Report of the Statutory Review of the *Enhancing Online Safety Act 2015* and the Review of Schedules 5 and 7 to the *Broadcasting Services Act 1992* (Online Content Scheme) (jointly referred to as Briggs Report), and now also the Draft Online Safety Charter.

Furthermore, triggered by the terrorist attack in Christchurch on 15 March 2019, further measures with respect to the removal of illegal online content may flow from the Prime Minister's Roundtable in Brisbane on 26 March 2019 and the new Taskforce to combat violent terrorist and extreme material online.

Against this background, it is not quite clear to us how the proposed Charter would engage with the measures that may flow from the Roundtable/Taskforce, the DPI and the

recommendations that are already contained in the Briggs Report. While the Consultation Paper states that "it is intended to articulate a set of community-led minimum standards for industry to protect citizens, especially children and vulnerable members of the community, from harmful online experiences", it is not clear what this would mean for industry, including ISPs, in practice or how those standards would be determined or measured. Is the intention of the Charter to supplement any gaps in existing legislation and regulation? In that case, it would seem prudent to let the relevant stakeholders deal with the respective recommendations of the initiatives and, subsequently, to address any remaining issues through the Charter.

Our industry supports, in-principle, the development of an Online Safety Charter. However, we are keen to get a better understanding as to what the Government intends the Charter to achieve that is not likely to be achieved through existing or future anticipated legislation and regulation.

Scope of the Charter

Our industry shares the desire to foster a dialogue between community, industry and Government about the shared responsibility for online safety. As highlighted in the Consultation Paper, the provision of online content involves many and diverse players that offer a wide range of products and services. While it may be tempting to summarise those players under the broad term of 'technology firms', this is not appropriate, given the vastly different roles that those players assume in making online content available to the community and given their very different capabilities to deal with harmful online content.

Therefore, we object to the use of the term 'technology firm' and strongly recommend to clearly spell out (and separate) the different roles and responsibilities for the individual players in this area. Otherwise, the Charter is likely to create community expectations that some players are technically or legally unable to fulfil.

More specifically, almost all of the Charter's proposals are aimed at content creators or hosts, media platforms or potentially search engines. Hardly any of the recommendations would apply to Internet Service Providers (ISPs), who have no ability to routinely identify, moderate, manage or remove harmful content from a website. Consequently, they should also not be held accountable for such content or be required to deal with complaints about such material. It is equally inappropriate to expect the freezing of accounts that end-users have with ISPs.

ISPs can – and do – block user access to websites that host harmful content where ISPs receive lawful requests from the responsible authorities/agencies to do so. Such blocking requests can be made by law enforcement agencies using the powers given to them in Section 313 of the *Telecommunications Act 1997;* for example, with respect to the blocking of sites which are part of the Interpol Blacklist. The use of Section 313 is subject to the *Guidelines for the use of section 313(3) of the Telecommunications Act 1997 by government agencies for the lawful disruption of access to online services*.

Search engines also delist websites from their index based on the Interpol Blacklist and the recently expanded *Copyright Amendment (Online Infringement) Act*.

It should be noted that website blocks must be very targeted to avoid over-blocking, i.e. the inadvertent blocking of websites that do not host harmful content. However, even where such blocks are correctly targeted, they only provide a partial solution to disabling access to content due to the large volume of ISPs (more than 400) in Australia and the complexity of requesting all ISPs to install a block. Moreover, site blocking is easily overcome by users that wish to access a blocked website through the use of VPNs, use of the Tor network or Tor browser, anonymous proxies, HTTPS access, SSH tunnels, remote desktop clients and purpose-built programs.

Consequently, the blocking of websites must be viewed as a means of last resort – but where it is required, it appears that existing legislation and regulation is able to facilitate such blocks.

However, we believe that it would be beneficial to establish clear communication, cooperation and coordination channels for emergency situations (such as the Christchurch terror attack) to ensure that Government agency/regulator direction is clear, and that action can be taken within very short timeframes and with a firm legal support.

Consequently, we welcome the establishment of the Taskforce to combat violent terrorist and extreme material online which brings together a range of Government stakeholders, relevant agencies and industry players.

We look forward to continuing our engagement with all relevant stakeholders on measures designed to create a fit-for-purpose, technology and platform-neutral framework for online safety.

Please contact Christiane Gillespie-Jones (c.gillespiejones@commsalliance.com.au) if you have any questions.

Yours sincerely,

John Stanton

Chief Executive Officer
Communications Alliance