COMMUNICATIONS
ALLIANCE LTD

COMMUNICATIONS ALLIANCE

Submission to the
Department of Social Services
IMPACT OF ILLEGAL OFFSHORE WAGERING REVIEW

November 2015

TABLE OF CONTENTS

INTRODUCTION

Communications Alliance appreciates the opportunity to provide a submission in response to the Department of Social Services Impact of Illegal Offshore Wagering Review.

ABOUT COMMUNICATIONS ALLIANCE

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.

1. SUMMARY

Communications Alliance members include Australia's major Carriers and Carriage Service Providers (C/CSPs) and Internet Service Providers (ISPs).

We welcome the opportunity to comment on the Department of Social Services Impact of Illegal Offshore Wagering Review (Review). The telecommunications industry provides the infrastructure that is used to access offshore wagering sites. The regulatory regime that applies to the industry includes a mechanism that has been used for blocking of illegal services. However, industry level blocking can be easily circumvented and, in our submission, is not a realistic and practical alternative to the development of coherent and internationally competitive industry policy.

We believe that for any scheme designed to address illegal offshore wagering to be sustainable, it must have a harmonised approach involving the local wagering industry and Government at both the State and Federal levels.

Possible action includes:

- harmonisation at a Federal Government level to address the diverse regulatory regime currently in place for gambling and wagering and the lack of a national regulator;
- as an initial step, increasing resources to enforce the current prohibitions expressed in the Interactive Gambling Act (2001) (IGA). Except in relation to micro-betting on sports other than horse and greyhound racing, provision of wagering services to Australians from offshore is not prohibited by the IGA.
- We observe that, expanding the scope of the prohibition under the IGA to include conventional wagering:
    a. must be properly resourced. It appears that enforcement of the current scope is not properly resourced and the existing restrictions largely go unenforced;
    b. would require consideration of any free trade obligations when attempting to restrict offshore wagering;
    c. would not be consistent with the recommendations of the Productivity Commission report on Gambling (2010) which suggested liberalisation as the best means to encourage the use of domestic services that pay tax and can be made to implement harm minimisation measures; and
    d. may be futile in any event for technical reasons (see discussion of VPNs below).
- resolution of funding for any scheme which may involve C/CSPs and ISPs in assisting other parties (particularly law enforcement agencies) to address other digital content issues.

Potential Unintended Consequences:

We urge careful consideration of any proposal to extend the use of Section 313 of the Telecommunications Act to require ISPs to block offshore wagering websites, as such use has the potential to capture many other entities, including schools, universities, libraries and cloud-based services in ways that may hamper their legitimate activities and disadvantage consumers. For further elaborations on the use of Section 313, please refer to the Communications Alliance / AMTA submission (Aug 2014) and supplementary submission (March 2015) to the House Standing Committee on Infrastructure and Communications' consultation on *Disrupting Access to Illegal Online Activities using the Telecommunications Act 1997*.

2. COMMENTS ON REVIEW QUESTIONS

Communications Alliance makes the following comments on selected questions from the Impact of Review discussion paper.

Question 3: What measures could be implemented to improve the enforcement of the Interactive Gambling Act 2001 and any other relevant legislation (Commonwealth, state and territory) including any enhancements to presently existing prosecution, investigation and complaints handling processes?

Whilst Industry has been approached to discuss the current regulatory regime for gambling and they are able to comment on observations, Industry would not see this as a matter they ought to be involved in. The primary involvement in gambling legislation which Industry have is through the Communications Alliance Interactive Gambling Industry Code developed by the former Internet Industry Association to comply with Section 36 (1) of the IGA.

Industry notes from its observations some of the areas the Review may wish to investigate are:

- Currently under the IGA the provision to Australians of gambling services – not wagering services – is made illegal. Accepting bets online after a sporting event has started (other than horse racing and greyhound racing) is banned but, as far as we are aware, no steps have been taken by any regulator to enforce this prohibition.
- Wagering is allowed in Australia, so by banning it for overseas operators, there may be implications under the free trade obligations resulting in potential private rights for overseas operators to claim compensation. The policy behind the IGA was not to cocoon Australian industry from the impact of competition from offshore, but to protect Australians from the increased risk of personal and social damage from online casinos. In circumstances where online wagering is permitted in Australia, a very clear case should be made before implementing changes to ban offshore providers.
- The diverse regulatory regime in Australia, which sees differences in legislation between some State and Territory Governments, along with the absence of a national regulator, may be an area worth considering prior to actually dealing with any issues posed by offshore wagering operators. Before prohibiting the provision of wagering services to Australians from offshore operators, Government should be satisfied that the regulatory regimes that apply to offshore operators are inferior to those under which Australian operators are licensed including in the Northern Territory and Norfolk Island.

Providers such as Google comply with relevant State/Territory legislation regarding obligations around paid advertising of gambling and wagering services. Advertising of these services is only permitted from advertisers who are licensed in Australia. In the case of Google, applications for posting online advertising are verified to confirm the validity of the body giving the authority and the business given the authority. Only recognised Government authorities are certified. Legal advice is sought to confirm any new Government authorities.

Question 4: Are there non-legislative options, such as technological and financial innovations, that could be implemented to limit the access to illegal offshore wagering sites by Australian based customers?

The blocking of websites is regularly considered by those outside the Industry as a solution to issues associated with illegal or fraudulent activities that take place on the internet. The Australian telecommunications industry has been willing to assist in the blocking of sites which are classed as the 'worst of the worst' (Interpol black list), and has been subject to requests for blocking of illegal content under Section 313 of the Telecommunications Act 1997.

The issues associated with the use of Section 313 have been considered recently by the House of Representatives Standing Committee on Infrastructure and Communications (see its report (*Balancing Freedom and Protection* issued on 1 June 2015).

The use of blocking to achieve social policy outcomes is problematic. Site blocking in general is a relatively blunt tool and has the potential to extend outside original intentions. (This was the case in the so-called ASIC-incident where the use of Section 313 of the Telecommunications Act to request blocking of a site also resulted in the inadvertent blocking of thousands of additional websites, refer to Sections 2.20 to 2.25 of the report *Balancing Freedom and Protection*).

Site blocking requires a request to be made to ISPs to actively block a domain name, and requires personnel with the necessary technological expertise to undertake the task. However, such blocks, even if correctly targeted, only provide a partial solution due to the large volume of ISPs (over 400) in Australia and the complexity of requesting all of them to install a block. If not all ISPs are part of the arrangement, there is the potential for wagerers to pick and choose their ISP so as to avoid any site blocking.

As with any type of scheme proposed to be introduced, there are processes required to be set in place and the question raised as to who pays for any enforcement scheme.

These concerns have already been raised in the aforementioned Communications Alliance / AMTA submissions to the 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*.

The below extract from the March 2015 submission outlines some of the procedural matters to be considered before a blocking scheme can be introduced:

"(…)

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 level of seniority of the authorising officer requesting the blocking of a website;
3. set out the limitations of liability on the part of the service provider;
4. require 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 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.

In addition to the above, (Communications Alliance and AMTA) support the development of an 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;
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."

In addition to the concerns raised above and in previous submissions, it should be noted that site blocking is easily overcome by users that wish to access a blocked service. VPNs encrypt the traffic between the user and the offshore site so that the local ISP is unable to determine the source or content of the traffic. VPNs have a legitimate place ensuring privacy and security of sensitive communications. There are a range of commercial VPN providers, e.g. vyprVPN, purevpn, overplay, HideMyAss, ipvanish, CyberGhost etc.

The importance of VPNs has recently been illustrated by a major uptake in VPN usage following the introduction of Australia's mandatory data retention regime, e.g. refer to http://www.cnet.com/au/news/vpn-use-increases-in-australia-amid-data-retention-and-piracy-concerns/ or http://www.theaustralian.com.au/technology/australians-flock-to-vpns-to-avoid-data-retention/story-e6frgakx-1227022957464?sv=72ec3f56f5b397bca342422c0b409afa/ or http://www.crikey.com.au/2015/03/27/data-retention-laws-will-get-worse-with-vpns-the-only-winners/.

Furthermore, Industry believe that there is merit in better-coordinated Government-driven education of consumers on the pitfalls of gambling and the potential dangers involved in using overseas providers.

The need for "a coordinated Government-led education campaign (…) to push and actively promote the safe(er) use of social media, email and the internet" is an area which has also been highlighted in the Communications Alliance submission made to the Department of the Prime Minister and Cabinet in March 2015 in response to the Cyber Security Review.

COMMUNICATIONS
ALLIANCE LTD

Level 12
75 Miller Street
North Sydney
NSW 2060 Australia

PO Box 444
Milsons Point
NSW 1565

T 61 2 9959 9111
F 61 2 9954 6136
E info@commsalliance.com.au
www.commsalliance.com.au
ABN 56 078 026 507