UNCLASSIFIED

AUSTRALIAN CRIME COMMISSION

OFFICE OF THE CHIEF EXECUTIVE

Our Ref: 14/144288
Your Ref:

Mrs Jane Prentice MP
Chair
House of Representatives Standing Committee on Infrastructure and Communications
Parliament House
Canberra ACT 2600

Dear Mrs Prentice

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

The ACC welcomes the opportunity to make a submission in response to the Standing Committee's Inquiry. The ACC supports the aim of implementing greater transparency and accountability mechanisms in relation to the lawful blocking of websites while maintaining the ability of Australia's law enforcement and national security agencies to prevent serious harm to the Australian community. It is critical that law enforcement and national security agencies maintain access to effective tools to prevent and disrupt criminal activity, particularly at a time when cyber technology is rapidly evolving and being used to facilitate an increasing range of criminal activity.

Section 313 of the *Telecommunications Act 1997* has proven to be a useful tool for Australian law enforcement to prevent harm to the Australian community caused by serious and organised crime from occurring. While it is not the only tool available to government agencies to use, it is an important tool nonetheless. To date it has been used successfully to address cases of child sexual abuse and serious financial crime such as transnational fraud – both of which have the potential to cause significant harm to Australia, its economy and its citizens.

The success of s.313 for the lawful blocking of websites relies upon private sector compliance with law enforcement requests. It is noted that failure to comply with a request to lawfully block a website pursuant to s.313 does not carry any consequences. In addition to the terms of reference being considered by this Inquiry, consideration could also be given to addressing this issue.

While increased transparency and accountability around the use of s.313 for the purpose of lawfully blocking websites is supported, this must not extend to requiring government agencies to reveal methodologies and operational strategies, particularly during active investigations. Balancing transparency, accountability and law enforcement effectiveness can be achieved by creating a regime that is proportional to the threat posed by serious and organised crime.

ACC HEADQUARTERS
44 Mort Street Canberra ACT 2601
GPO Box 1936 Canberra ACT 2601
Tel: (02) 6243 6613 | Fax: (02) 6243 6679 | Internet: www.crimecommission.gov.au

(a) Which government agencies should be permitted to make requests pursuant to section 313 to disrupt online services potentially in breach of Australian law from providing these services to Australians

The online environment continues to be exploited by criminal elements on a daily basis, using new and increasingly sophisticated techniques to conduct their illicit activities and target the Australian community. For example, online marketplaces such as Silk Road provide an avenue to sell and purchase illicit commodities. Criminals are increasingly using new and converging technologies—including the Internet and Internet based platforms—to facilitate crimes such as identity theft, money laundering, mass marketing fraud, credit card fraud and the sale of illicit or counterfeit goods.

The ACC submits that detailing specific agencies permitted to make requests pursuant to s.313 for the purpose of lawfully blocking websites is potentially limiting, particularly in the face of these technologies advancements. Arbitrarily specifying agencies will artificially restrict the ability of the Australian Government to combat criminal activity conducted online, and will not enable flexible responses to the inevitable evolution of the online landscape.

Rather, the power to disrupt online services potentially in breach of Australian law should be focused on the type, characteristic and proportionality of the activity being conducted, or importantly, facilitated. This approach would ensure that any agency with a clear need can access the powers to block websites.

In doing so, any government agency with responsibility for addressing serious criminal activities, organised crime or national security is automatically afforded the power to lawfully block websites that expose the community to harm.

(b) What level of authority should such agencies have in order to make such a request

The ACC submits that staff investigating a relevant offence could submit a written application to an authorised officer – agency head or his/her delegate – their agency setting out the case for implementing a website block. The application would detail the facts and circumstances of the case and the offences being investigated, similar to a subpoena or summons application.

(c) The characteristics of illegal or potentially illegal online services which should be subject to such requests, and

Restricting access to Section 313 for the purpose of lawfully blocking websites based on a limited list of defined offences will not provide agencies with sufficient flexibility to be able to respond to newly emerging, innovative or novel crime types.

An appropriate definition needs to ensure disruption of online services can encapsulate current or future criminal activities, but is balanced so as not to undermine freedom of expression by the community and remains proportional to the threat. Currently, subsection 313(3) carriage service providers are required to give officers and authorities of the Commonwealth and of the States and Territories such help as is reasonably necessary to:

- enforce the criminal law and laws imposing pecuniary penalties

- assist the enforcement of the criminal laws in force in a foreign country
- protect the public revenue
- safeguard national security

The current definition remains relevant, capturing the type and characteristic of activity to ensure agencies are able to respond to newly emerging, innovative or novel crime types. However, recognising the extent of power to disrupt online services s313 provides, there is merit in considering the proportionality of the activity being conducted or facilitated.

For example, the definition of *serious and organised crime* as defined in the *Australian Crime Commission Act 2002* means an offence that, inter alia, involves substantial planning and organisation; and involves, or is of a kind that ordinarily involves, the use of sophisticated methods and techniques. This provides the proportionally threshold that strictly limits the ACC in the type of investigations or intelligence operations it can conduct.

Similarly, other legislation also provides for proportionality thresholds to ensure flexibility for law enforcement agencies, but balanced with protections for the community.

By incorporating a proportionality threshold, s313 would provide response agencies with sufficient flexibility to respond to a wide range of criminal or national security threats while at the same time creating a sufficient access threshold to ensure the proportionality of responses. This will ensure that s.313 powers for the purpose of lawfully blocking websites can only be used in response to the most serious threats impacting the Australian community.

(d) What are the most appropriate transparency and accountability measures that should accompany such requests, taking into account the nature of the online service being dealt with, and what is the best/appropriate method for implementing such measures:

a. Legislation
b. Regulations, or
c. Government policy

It is important to note that while accountability and transparency are important, there is also a legitimate need for law enforcement and national security agencies to retain a level of secrecy in order to ensure the integrity of current and future operations.

On this basis, agencies should not be required to publically release certain information relating to the use of s.313 powers for the purpose of lawfully blocking websites where it could, inter alia, expose sensitive sources and methodologies employed by law enforcement and national security, impact the safety of individuals, or publically expose active investigations or classified intelligence.

Notwithstanding this, the ACC supports a consideration of a formal transparency and accountability regime in relation to the use of powers contained in Section 313 to ensure the maintenance of public confidence in government agency use of these powers, incorporating protections outlined above. This regime could include a suite of measures legislative or policy measures including:

- The development of a publically available whole-of-government policy and information package that clearly states policy objectives and protections.
- A formal, consistent and documented application and approval process.
- An appeals mechanism could be considered and the use of notification pages to inform internet users that a website they are seeking to access has been blocked, could also be

considered on a case-by-case basis.

- A central entity with responsibility for publishing information on the regime and dealing with disputes and appeals, and reporting of the use of s.313 blocks. Reporting could mirror the *Telecommunications (Interception and Access) Act 1979* Annual Report.

The ACC considers that these accountability and transparency mechanisms achieve the desired balance between the need for response agencies to maintain adequate flexibility to prevent harm to the Australian community, and the need to provide reassurance to the general public that powers entrusted to Australia's law enforcement and national security agencies are being used appropriately.

Should your office require further information please have them contact Nathan Newman on (02)6243 6657 or via email to nathan.newman@crimecommission.gov.au.

Yours sincerely

Chris Dawson APM
Chief Executive Officer
27 August, 2014