UNCLASSIFIED

AFP
AUSTRALIAN FEDERAL POLICE

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

House of Representatives Standing Committee on Infrastructure and Communications

Background

The Australian Federal Police (AFP) welcomes the opportunity to make a submission to the *House of Representatives Standing Committee on Infrastructure and Communications* (the Committee) in relation to the use of subsection 313 (3) of the *Telecommunications Act 1997*, which obliges carriers and carriage service providers to provide assistance to Commonwealth, State and Territory agencies to uphold Australian law.

The AFP only uses section 313 to disrupt illegal online activity where other mechanisms to prevent the activity have been or are unlikely to be successful. The AFP currently utilises section 313 requests to prevent access to websites which distribute child exploitation material and for cybercrime related matters.

Criminal groups are continuously looking for opportunities to exploit technology in order to commit crime and to counter law enforcement efforts. For example, websites that are used to host child exploitation material or malicious software, or are used for the illicit sale of narcotics and firearms, are generally hosted outside of Australia's jurisdiction and in countries where police to police assistance or the Mutual Legal Assistance framework is unlikely to be effective. Section 313 provides an additional tool for law enforcement, national security and regulatory agencies to disrupt such serious crime in a rapidly evolving technological environment.

AFP response to the Terms of Reference

In response to the TOR the AFP provides the following information for the Committee to consider:

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 Australia

The AFP submits that blocking under section 313 provides law enforcement, national security agencies and regulatory bodies with an effective tool to prevent and disrupt activity which may cause serious harm to the Australian community.

Section 313 provides the AFP with a proactive means of blocking criminal content, in order to disrupt and prevent online illegal activity and the commission of serious offences against Australian law.

Whilst it is a matter for the Committee to consider, the AFP recommends that section 313 should be available to law enforcement, government agencies and regulatory authorities which have statutory responsibility to address serious and organised crime and matters of national security.

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

Historically, section 313 blocking requests within the AFP have been authorised by a Commissioned Officer (Superintendent or above). The level of approval has been commiserate with the seriousness of the crime and the level of disruption activity.

The AFP recommends that future section 313 blocking requests continue to be considered and authorised by a Commissioned Officer (Superintendent or above).

The AFP believes that this level of internal authorisation provides for an appropriately senior level of accountability and oversight. The AFP believes that similar internal authorisation should be the standard for the other Government Agencies using Section 313 for blocking.

c) the characteristics of illegal or potential illegal online services which should be subject to such requests, and

Between June 2011 and August 2014 the AFP has issued twenty-three section 313 requests for the purposes of blocking websites used for illegal online activity. The majority of these requests were made to support the blocking of Interpol's 'Worst of List' in relation to online child exploitation material.

Given the pace of technological change and the prevalence of criminal activity being conducted or facilitated online, it is important that section 313 continues to provide law enforcement agencies sufficient scope to engage with service providers to prevent the commission of serious criminal offences. Offences that are not currently committed online could in the future transition to the online environment as a result of technological changes.

The AFP is currently utilising section 313 requests to prevent the following illegal activity:

<u>Online distribution of child exploitation material</u>

In 2009, the Interpol General Assembly adopted a resolution which sought to reduce the increasing rates in online access and distribution of child exploitation material (CEM), through the use of all available technical tools, including internet access blocking.

The primary purpose of the internet access blocking is to prevent the access to CEM and to deter people from further access to CEM.

The internet access blocking promoted by Interpol operates at the Internet Service Provider (ISP) Domain Name Server (DNS) level. The websites on the 'Worst of List' have been detected as containing the most severe CEM. The 'Worst of List' list is provided to national police agencies for distribution to domestic ISPs in accordance with local legislation and policies.

The AFP has used section 313 requests to block access to Interpol's 'Worst of List' of child exploitation websites. The AFP facilitates the dissemination of the 'Worst of List' and does not make alterations to the contents. Should the AFP become aware of a website that should be included, or removed from the 'Worst of List', then the relevant information is provided to Interpol for assessment as detailed in the inclusion criteria.

To be included in the 'Worst of List' domain names or websites must meet the following criteria:

- Contain images and/or video
- The children are 'real'. Sites containing only computer generated, morphed, drawn or pseudo images are not included
- The ages of the children depicted in sexually exploitive situations are (or appear to be) younger than 13 years
- The abuse is considered severe, depicting sexual contact or focus on the genital or anal region of the child
- The domains have been online within the last three months
- The domains have been reviewed and found to fulfil the above criteria by two independent countries/agencies or more.

The above criteria have been designed to ensure any material which meets the criteria can be considered illegal material in all Interpol member countries. When an Australian user attempts to access a website contained on the 'Worst of List', they are redirected to an Interpol 'Stop Page', which states their access has been blocked as it contains child sexual abuse material. The purpose of the redirection or 'Stop Page' is purely preventative, and is not used for investigative purposes.

An AFP review of the Access Limitation Scheme in January 2012 concluded that the redirection at the DNS level had no adverse effect upon the speed, capacity or capability of the participating ISP's network. In addition, the Access Limitation Scheme appeared to have caused a reduction in the access of CEM via the internet.

The AFP believes blocking this known criminal content is a proactive, disruptive and preventative strategy which is a positive step in helping to protect children from sexual exploitation and abuse.

Cybercrime

In early 2014, the AFP utilised a number of section 313 requests to prevent the distribution of peer-to-peer malicious software (malware) which was designed to steal personal banking and financial credentials from the platforms of Australian computer users.

The AFP was aware that the domain supporting the malware was used for the exclusive purpose of distribution and updating the malware.

The blocking by ISPs of this domain prevented the widespread distribution of this malware in Australia and the subsequent compromise of Australian's financial details that potentially could have been used to undertake large scale fraud.

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

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

There is currently no specific oversight on the use of Section 313 governed by the Telecommunications Act 1997. The AFP's use of section 313 is subject to existing internal and external governance procedures. This includes complaint mechanisms through the Commonwealth Ombudsman, ACLEI and external scrutiny by Parliamentary Committees which current AFP procedures such as Controlled Operations are subject to.

Section 313 provides the AFP with an effective means to disrupt illegal online activity where other mechanisms to prevent the activity have been or are unlikely to be successful. The AFP considers its use of Section 313 to block internet content has been reasonable and proportionate to the threat of the criminal activity.

The AFP recognises the need to demonstrate accountability and transparency in respect of the use of section 313 requests in order to maintain public confidence that blocking powers are being used proportionately and appropriately.

The AFP supports the development of whole of government policy objectives and information, which sets out a threshold for access to section 313 and the relevant serious offences.

The AFP would welcome annual reporting on the number of blocking requests made under section 313 for the purposes of disrupting illegal online services through a central body. However, considers releasing specific details publicly as to the nature of each individual request and to which ISP each request was made may have a substantial adverse effect on the proper and efficient operations of the AFP and may be contrary to the public interest.

Conclusion

The AFP recognises the need to display transparency and accountability in relation to section 313 blocking requests. Criminal elements actively seek to subvert law enforcement and national security efforts to counter their activity and section 313 requests provide government agencies with an additional tool to prevent the commission of serious crime online.