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

On 13 March 2015, the Australian Federal Police (AFP) received a letter from the Standing Committee on Infrastructure and Communications seeking a response to a number of questions that were raised following subsequent hearings.

In response to these questions the AFP provides the following:

1) **From the AFP's point of view, what are the principal purposes of disrupting illegal online services – catching criminals, preventing access, reducing levels of casual or inadvertent contact, education or other – and what is the level of disruption you are trying to achieve?**

There are multiple layers and complexities with respect to the use of disruption activities by Law Enforcement and it is difficult to categorise all operational activities relating to s313 within a single purpose. Outcomes based on s313 activities can range from the prevention of accidental exposure to Child Exploitation Material through to effective Cybercrime dismantling of Malware command and control networks. In each case Law Enforcement recognises that there are means for circumvention but the effects can be wide ranging depending on the situation.

Child Protection

The principle purpose of the AFP's use of section 313 in respect of child protection is to prevent access to Child Exploitation Material (CEM) and to reduce the levels of casual or inadvertent contact a person may have to this material.

It is difficult to quantify the level of disruption this will achieve; however, currently the access limitation scheme covers approximately 82% of private consumers in Australia utilising an Australian Internet Service Provider (ISP).

In the past decade, there has been exponential growth in the use of the internet and the availability of CEM online. In this environment, the AFP must prioritise its limited investigative resources towards investigations that will have the greatest impact in identifying offenders and removing children at risk from harm. This includes investigations in relation to offenders that sexually abuse children, profit

from the trading of CEM, or facilitate the sexual and physical abuse of children through online video streaming.

The AFP utilises the access limitation scheme as one technique to prevent access to CEM online.

Cyber Crime

In April 2014 the AFP utilised two section 313 requests to block domains which were believed to be used to update the Game over Zeus (GoZ) malware. In this circumstance the purpose of the section 313 request was to protect Australians from possible financial loss by rendering the malware ineffective. This action, was one part of a Federal Bureau of Investigations (FBI) led global take down of the GoZ malware.

The use of s313 in this case is extremely effective as, unlike in the case of CEM where an individual can take subsequent steps to avoid website blocking, malware is limited in its ability to dynamically respond to a loss of command and control infrastructure. This can therefore render networks of malicious software ineffective, dependant on their objectives. Whilst this will not prevent cybercriminals from conducting further damage, it does mean that they need to start again and rebuild their network.

2) Given the ease with which the blocking of websites can be circumvented, is the disruption of illegal online services worthwhile? How is it made effective?

As previously noted the ease of circumvention of blocked websites is relevant to a subset of criminal investigations conducted by the AFP. Whilst the AFP acknowledges that if a person has a genuine desire to access CEM that they may utilise other methods to circumvent the blocking of illegal online services. The AFP submits that the access limitation scheme is not capable of, nor intended to, capture all persons attempting to access CEM. Blocking of illegal online services is one of many disruption strategies undertaken by law enforcement.

The AFP believes that the disruption of illegal online services is an effective tool in preventing access through Australian ISP's to CEM.

The AFP, with its domestic and foreign law enforcement partners, utilises other methods and investigative strategies to identify those attempting to access CEM through Virtual Private Networks or networks such as TOR.

When taken out of the context of preventing a person from accessing illegal material and instead contextualised with respect to preventing or restricting systems infected with malicious software access to command and control networks it is an extremely valuable and worthwhile activity. The end result of effectively removing command and control can lead to the inability of viruses

aimed at stealing banking credentials from supplying those credentials to the persons controlling the software.

3) Concerns have been raised that s.313, as originally drafted, was not intended for the blocking/disruption of illegal online activity. Does the AFP have any concerns about the legal basis of using s.313 to disrupt illegal online services?

The AFP does not have concerns with the legality of carriage service providers' disruption of illegal online services in response to requests that invoke s313 of the Telecommunications Act. In the AFP's view there is nothing in the terms of the various obligations contained in s313, the drafting history of that provision and its predecessor provisions, or the explanatory memoranda that accompanied the enactment and amendment of those provisions from which to infer that the obligations s313 imposes do not encompass blocking of illegal online activity.

Rather, those various sources indicate that s313 and its predecessor provisions were expressly drafted in broad terms, and that broad formulation has been maintained through various statutory amendments over the course of the provision's history.

The AFP has reviewed the submissions to which the Committee refers in its letter in relation to this point. The arguments presented in those submissions have not altered the AFP's position on the issue.

4) Could the actions currently being carried out under s.313 be carried out more properly under other legislation, e.g. criminal law?

We assume this question to be asking whether the same objectives as those the AFP seeks to achieve by invoking companies' obligations under s313 might be achieved by other means, for instance criminal prosecution.

While it is open to the AFP to pursue criminal charges against site hosts, ISPs or end users for certain offences in appropriate circumstances, the decision whether or not to do so in a given case depends on various considerations. Those considerations include whether the AFP has jurisdiction over the person the subject of the proposed charge (which can depend on whether the person in question is within Australia's territorial jurisdiction), the severity of the conduct, the resources it would take to pursue the charge, the resources available to the AFP and the availability of evidence.

In many cases the illegal online content that requires blocking is hosted in foreign jurisdictions, and in some cases jurisdictions with which Australia does not have well established mutual assistance arrangements. In such cases, online content could feasibly be accessible to the Australian public indefinitely with very limited

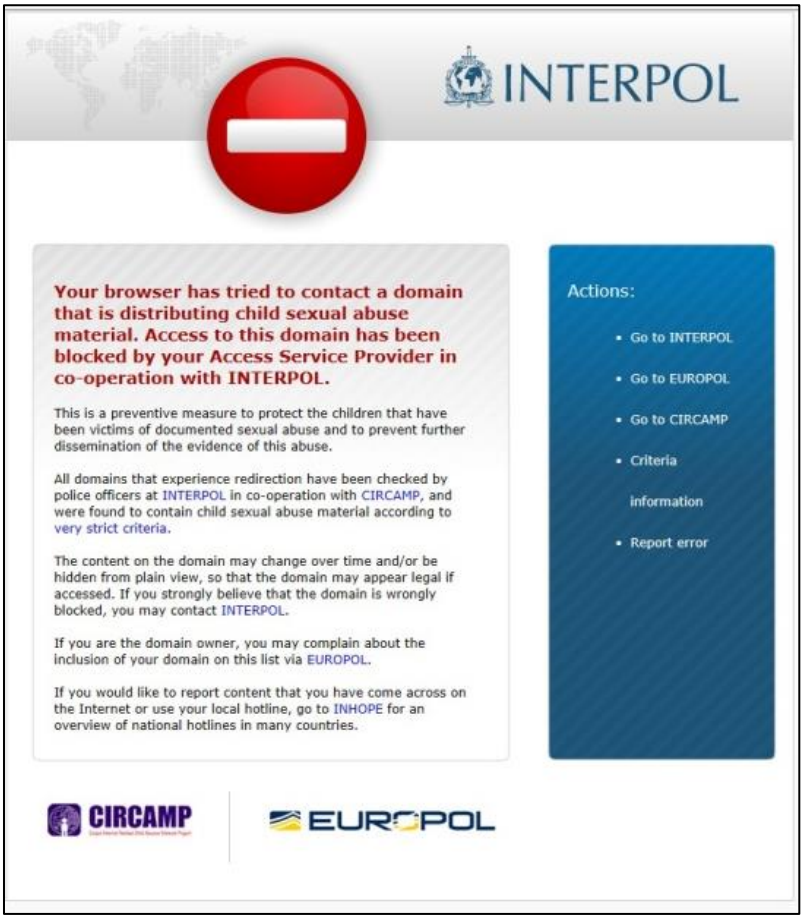
means by which Australian agencies can attempt to have such illegal content removed.

5) Does the AFP use block pages to alert users to the fact that a page has been blocked, by whom and why?

Interpol provides a generic 'stop page' that an ISP can choose to display to their customer. Use of the 'stop page' is not mandatory and an ISP may prefer to display an error message instead. Interpol recommends the use of the 'stop page' to increase transparency.

The 'stop page' advises the user that their browser has tried to contact a domain that is distributing child sexual abuse material. The 'stop page' provides avenues for a user to report online content and to make a complaint if they believe that the domain is wrongly blocked.

Below is an example of what a user would see if they attempted to access a blocked site using the Telstra network.



(Source: Attempted access to a blocked website through the Telstra network, 16 March 2015)

6) Have prosecutions eventuated from the blocking of websites?

The AFP has not prosecuted any person as a result of a section 313 request to block a website. The AFP does not access any data held by the ISP in relation to users who have attempted to access blocked websites.

7) Has the AFP ever been involved in the inadvertent blocking of innocent websites?

The AFP has not been involved in any inadvertent blocking of websites.