iiNet Limited
ACN 068 628 937

iiNet Limited
502 Hay Street
Subiaco, WA 6008

Support: 13 22 58
Sales: 13 19 17
Fax: 1300 785 632
Web: iinet.net.au

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

Introduction

iiNet is Australia's second largest DSL Internet Service Provider (ISP) and the leading challenger in the telecommunications market. We maintain our own super-fast broadband network and support over 1.8 million broadband, telephony and Internet Protocol TV services nationwide.

Thank you for the opportunity to provide a submission to the House of Representatives Standing Committee on Infrastructure and Communications in relation to its Inquiry into the use of section 313(3) of the Telecommunications Act (Telco Act) "to disrupt the operation of illegal online services".

The Committee has been asked 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 Australians;
>
> (b) what level of authority should such agencies have in order to make such a request;
>
> (c) the characteristics of illegal or potentially illegal online services which should be subject to such requests, and
>
> (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.

Necessary and proportionate

The principles of necessity and proportionality are a useful guide in determining:

- which government agencies can make requests pursuant to section 313;
- what illegal or potentially illegal online services (content) should be subject to such requests.[i]

iiNet has significant concerns with the use of section 313 to request service providers to block websites.

The scope of the obligation for providers like iiNet to do their "best" and to give help that is "reasonably necessary" is vague and uncertain. The provision appears to unfairly put the onus of testing the validity of the request on the service provider. iiNet believes that 'doing our best' is not limited to an unthinking, but efficient, supply of information but also requires us to apply our 'best' interpretation of our obligations under the legislation as well as 'doing our best' to consider any relevant implications for our corporate and social responsibilities. We do not believe that it is 'doing our best' to resort to guessing or hoping that agencies will use this power responsibly.

The widely-reported[ii] and controversial use of section 313 by ASIC, which led to an inadvertent "over-blocking" of some 250,000 websites[iii], is just one example of how the exercise of this power may contravene the principles of necessity and proportionality. Reportedly, ASIC:

> *asked internet service providers (ISPs) to block sites, it believed were defrauding Australians, by [blocking an] IP address (such as 203.56.34.11) instead of [blocking a] domain name (such as sitedefraudingaustralians.com).*[iv]

This Inquiry has been described as an inquiry into the use of section 313**(3)** by government agencies to disrupt the operation of illegal online services. It is not helpful to focus only on sub-section (3) of this power. Previously some agencies, including the AFP, have sought assistance from ISPs under sections 313**(1)** and 314 (rather than section 313(3)) to limit the operation of illegal online services. The Committee's own discussion of this Inquiry is not clear. As section 313(1) is a "prevention" obligation it could be seen as more appropriate to rely on this provision to block and disrupt facilities from being used in the commission of serious criminal offences, such as child sexual abuse and exploitation.

Sections 313(1) and 313(3) are vague, uncertain and overlapping:

- s.313(1) is about "preventing" criminal offences. It requires a carrier/CSP to do its "best" to "prevent" networks/facilities from being used in, or in relation to, the "commission of offences"
- s.313(3) is mainly about "enforcing" laws. It requires the carrier/CSP to give "such help" as is necessary" for various defined purposes including "enforcing the criminal law".

It is inappropriate that an ISP like iiNet cannot easily determine what its obligations are under either section 313(1) or 313(3). ISPs should not be placed in a position where they have to make difficult decisions or seek legal advice about what its obligations are under section 313. The decision making on when "help" is required of ISPs should ideally be made by a court. iiNet's internal site blocking policy resolves this uncertainty by imposing a number of tests which must be passed before a decision can be referred to the Chief Regulatory Officer for approval to commit resources.

Section 314 allows a carrier or CSP to recover its costs (and agree other terms) for providing "help" under section 313**(3)**. Costs should also be recoverable for assistance provided under section 313**(1)**. Agencies themselves seem to be confused about the interaction between sections 313 and 314. For example, iiNet has received a request from an agency which sought assistance under section 313**(1)** and then set out the terms of assistance applicable pursuant to section 314. However, section 314 relates only to help provided under section 313(3), not assistance provided pursuant to 313(1). In

this context, iiNet urges the Committee to consider these issues holistically and clarify the obligations under both sub-sections (1) and (3) of section 313 as well as the scope of section 314.

Who: a narrower set of government agencies

The current wording of section 313 is too broadly framed as to the almost unlimited range of government and law enforcement agencies that can rely on the powers set out in section 313 namely "*officers and authorities of the Commonwealth and of the States and Territories*". The use of section 313 should be restricted to a far narrower range of the critical law enforcement, anti-corruption and national security agencies that have a demonstrated need for such a power to block online services. It would not be necessary or proportional, for example, for local councils to be able to rely on section 313(1) or (3) to request an ISP to block a site.

What: type of content – "serious contraventions"

Section 313 should only be used in cases of "serious contraventions" of the law, as defined in the *Telecommunications (Interception and Access)* Act.[v]

The Inquiry should also seek to reduce any duplication between section 313 and existing "take-down" style powers in other legislation. For example, there are existing powers under the *Broadcasting Services Act 1992* where the ACMA can issue take-down notices concerning sites hosted in Australia that contain "online prohibited content". There are also existing take down powers in relation to content that might be infringing copyright in the Copyright Act and regulations. These existing powers should be taken into account when considering:

- what agencies can use section 313 and
- what type of illegal content should be covered by section 313 site blocking powers.

The Committee should also consider how useful the site blocking powers under section 313 are from a technical perspective and whether alternative legal or practical approaches should be prioritised. The AFP's Deputy Commissioner Michael Phelan has said:

> *Over time, it's much more useful and far more valuable to actually get in contact with those that are hosting the material, and so on, and block it at the source, and get them to just tear down the sites, and so on, off-shore … .*[vi]

How: Standard approach, accountability and oversight

iiNet submits that any request to an ISP pursuant to section 313 powers to block websites must be accompanied by a court order. The court order should be sent to all ISPs not just two or three. Requiring only a small section of the industry to block sites will be ineffective and therefore, creates unnecessary costs for those required to implement blocks.

If the Inquiry is persuaded that a requirement for a court order is not necessary, then a section 313 request to block a site must at least be authorised by representative of an agency that has a level of seniority and accountability that is clearly prescribed in the Regulations.

iiNet has developed an internal Site Blocking Policy which could provide an appropriate framework in considering such requests and for this Committee in its Inquiry into section 313.

iiNet does its best to achieve an appropriate balance between complying with its legal obligations, to action requests from agencies to block websites, and ensuring that such requests are legally justified. In summary our Site Blocking Policy provides:

- iiNet will block sites only where external requests for compliance with legal obligations are supported by legitimate authorisation, appropriate legislation and due process.
- A request which does not meet the minimum criteria outlined in the policy will be declined.
- Any request that meets the requirements of this Policy must be approved by an iiNet executive before a site block can be implemented.
- While the obligations in section 313 are broad, iiNet must do its best to test all such requests to ensure that they meet reasonable standards.
- iiNet does its best by insisting that requests for the blocking of sites also provide (at a minimum):
  - personal contacts of the requestor in the relevant Authority;
  - transparency measures such as:
    - a redirection page with details of the reasons for the block and appropriate remediation or appeal processes for the affected parties;
    - evidence that the site contains prohibited content and/or is the subject of a relevant court order or judgment.

A standard approach for section 313 requests to block sites should not be left up to agencies and ISPs' own policies but should be set out in Regulations. This standard approach could include the following:

- what specific agencies can use this power;
- that a court order is required before sending a request;
  (or alternatively, setting out the level of authority within the agency that is required)
- the content of notices that appear on redirection pages when a blocked site cannot be accessed;
  (these notices would have the branding of the relevant agency, not the ISP)
- a mechanism for the site owner to appeal to the requesting agency, a relevant court or tribunal if they wish to challenge the blocking of the site.
- a mechanism for a site owner to apply to the requesting agency for removal of the block, where a legitimate website has been compromised, and the offending material has been removed.

Legislation should also provide for specific oversight and transparency measures such as requiring the relevant government agencies to inform the Department of Communications of their use of section 313 to block websites each January and June.

iiNet welcomes any questions from the Committee relating to this submission or the terms of Reference for this Inquiry more generally.

Stephen Dalby
Chief Regulatory Officer
iiNet Limited
e: sdalby@staff.iinet.net.au
ph: 08 9213 1371

Leanne O'Donnell
Regulatory Manager
iiNet Limited
e: lodonnell@staff.iinet.net.au
ph: 03 9811 0042

References

[i] For a further elaboration of these principles, we draw the Committee's attention to the *International Principles on the Application of Human Rights to Communications Surveillance*, available at: https://en.necessaryandproportionate.org/text

[ii] **For example:** ASIC's accidental block exposes secret internet filtering scheme, 16 May 2013, ZDNet, available at: http://www.zdnet.com/asics-accidental-block-exposes-secret-internet-filtering-scheme-7000015477/

[iii] Proof the internet filter lives on by other means, 16 May 2013, ABC The Drum, available at: http://www.abc.net.au/news/2013-05-16/westendorf-and-atahan---internet-filter/4694252

[iv] How ASIC's attempt to block one website took down 250,000, 5 June 2013, SMH, available at: www.smh.com.au/technology/technology-news/how-asics-attempt-to-block-one-website-took-down-250000-20130605-2np6v.html

[v] Definition of "serious contravention": http://www.austlii.edu.au/au/legis/cth/consol_act/taaa1979410/s5e.html

[vi] ASIC uses internet site blocking power 10 times in one year, 4 June 2013, ZDNet, available at: http://www.zdnet.com/au/asic-uses-internet-site-blocking-power-10-times-in-one-year-7000016371/