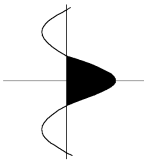
J & J Denham

GEOPHYSICAL CONSULTANTS Farmers & Graziers



11th August 2014

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

Section 313 of the Telecommunications Act 1997 has been around for a long time, and the wording of the section does not appear to have contemplated its use to block internet access to websites (which were in their infancy when the act was passed). In fact, the wording would seem to have been lifted from much earlier legislation and aimed purely at telephone/fax/telex communications.

As such, it would seem appropriate to look very closely at whether in fact this section should be used to disrupt the operation of illegal online services, or whether the wording should be clarified by amendment to the Act, either to specifically allow this use or to prevent it, and if to allow it, to specify how it should be used, although the details could be in regulations. Using a tortured interpretation of an act for a purpose that was not envisaged when it was passed does no service to Parliament.

There are several aspects that need to be considered when deciding this, and what action is needed.

- Will it work?
- What is the ethical situation?
- How do these considerations apply to the terms of reference?

Will it work?

To decide this, it is necessary to understand the structure of the internet, and specifically the Worldwide Web. If I click on a link to a web page, or type a URL (Uniform Resource Locator) address into a browser, this address (e.g. www.aph.gov.au) goes to a DNS (Domain Name System) server, where it is translated into an IP address for the particular server that holds that website, (e.g. 164.75.1.2), which is then contacted. The only tools available to an RSP to block access, without installing an obtrusive and expensive filtering system is to either modify their DNS server to redirect the request to a "block page" (DNS poisoning), or alternatively to block a specific IP.

Both of these options have serious defects. The first is that there is no obligation whatever for a customer to use their RSP's DNS server – there are many thousands of these available worldwide, and the user can easily change to another one, perhaps specifically to access blocked websites, or perhaps to an overseas DNS server that has extensive blocking – but not the ones blocked by the Australian s313 requests, or simply one that works more reliably than their RSP's DNS server (my RSP several months ago suggested users change to a different one to try and resolve certain issues).

If the IP address is blocked, and this appears to be the method used by RSPs to date under S313 requests (although with the secrecy that cloaks the process, this is by no means certain), it immediately runs into two problems. The first is that changing the IP address of a website to get round the block is trivial for the website owner (simply move to a different server), making the block ineffective, and the second, perhaps more important, is that a single IP address does not necessarily (indeed not usually) represent a single website. The extensive use of the system under the previous government came to light when a rather clumsy block of a financial scam page inadvertently blocked an estimated 20,000 unrelated websites, at least one of which was that of a fairly major educational institution. IP blocks are regularly used by RSPs to block emails coming from blacklisted IPs that have generated a lot of spam.

But both methods (IP blocking and DNS poisoning, or indeed any other method that can be envisioned) also suffer from the defect that it

is trivial to bypass them by routing the request through an overseas server using a VPN (Virtual Private Network). This is impossible to prevent and still allow, for example, business and financial systems of today to operate, as has been realised by repressive regimes worldwide. The tools to do this are widely available, and easy to use. This can also be done secretly, using tools provided by the Tor Project, which is funded by the USA government to allow citizens of repressive regimes to have unfettered access to the internet.

So the conclusion has to be that blocking under s313 will not really work, in that anyone who really wants to access these pages will have no trouble in doing so, and the only people blocked will be those who are not interested, or those who suffer secondary damage due to the use of IP blocks. And any owner of a blocked website can unblock it simply by changing to a different IP address or slightly changing the URL if DNS blocking is used. In summary, blocking websites is marginally effective, and can have (and has had) serious “collateral damage” effects out of all proportion to anything achieved by the block.

What is the ethical situation?

It needs to be remembered that this legal basis for blocking web pages was dreamt up by the previous government as a method of applying internet censorship without passing legislation after it became clear that the chances of such legislation passing through parliament were zero. In other words, it is a clear example of a government acting to circumvent the “will of the parliament”, something that one would hope would be rejected by the present government.

The present mode of use of the section provides the government (and indeed its agencies) with the opportunity for “secret censorship” (and we have no idea how extensive this censorship is currently!). Is this not the basic formula for establishing a police state? At the same time, it is an open invitation for corruption – if there is a website that, for example, is offensive to the government, what is there to stop the government, or an individual government (or opposition!) sympathiser (or someone who has been paid to block a certain website for business 'dirty tricks') at quite a low level, from simply organising a s313 request? As it stands there is no oversight whatever, and apparently

no restriction on which government employees can originate such a request.

Blocking access to information for citizens without their knowing what is blocked and why it is blocked will appear to most Australians to be quite unethical – it smacks of "Big Brother Knows Best" and is contrary to the principals of the various Australian censorship legislation. But there is a dilemma – as discussed above, it is impossible to effectively block any website from someone who wants to access it, so publishing what is blocked becomes a ready address list for anyone who wants to see what the government is stopping them from seeing. But is this a sufficient reason to tell Australians they can't know what the government does not want them to see?

How do these considerations apply to the terms of reference?

(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

In view of the wording of the Act, it seems to me pretty clear that the only agencies that should be permitted to make requests are police services and security services, seeing that the only reasons allowed are criminal or security matters, although one has to question what could be meant by "protect the public revenue" - does this mean that websites offering tax advice can be blocked?

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

To ensure that requests only meet the criteria:-

(c) enforce the criminal law and laws imposing pecuniary penalties;

(ca) assist the enforcement of the criminal laws in force in a foreign country;

(d) protect the public revenue; or

(e) safeguard national security.

It is reasonable to ask that the request be approved by someone outside the agency making the request, otherwise the bar is extremely low. Since most requests could be assumed to refer to criteria c, ca, d, then it seems to me that approval by a magistrate is appropriate. And

unless the agency can convince a magistrate of the need for secrecy, the request and the reason for it must be made public. Even if secrecy is approved there should be a regular, perhaps annual report on the numbers of these secret requests, and where possible a time limit on the secrecy applied.

Except in exceptional circumstances, a block should redirect to a page showing that it has been blocked by the government, and is not inaccessible for technical reasons, otherwise the government will soon be taking the blame for any technical problem that makes a website inaccessible!

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

Since, as discussed above, it is impossible to effectively block anything, and because of the potential for disruption to unrelated websites, great care is needed in deciding what websites are suitable for these requests.

The ease with which the blocks are avoided would suggest that the tool should only be used only where a temporary blockage would be effective, for example, where there is evidence or a strong suspicion that a website is being used to direct or conduct a criminal activity, and there is already action in progress or planned to combat this. This might include a child pornography website, allowed to continue operation to avoid alarming the perpetrator while police in the site's home country track down who is really behind it.

Use of requests to block websites that would be the subject of a takedown order if located in Australian jurisdiction is almost certainly not a good idea, as the number of these is so large that the collateral damage would soon bring the Australian internet to its knees and make Australia a world laughing stock. Or alternatively, this criteria would only be applied selectively, which again opens the opportunity

for corruption, where police officers could fail to notice where suitable rewards were available. A selectively enforced law is a bad law.

(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:

As discussed above, the primary measure to ensure transparency and accountability is to require that requests be approved by someone outside the requesting agency, and that the request be made public. As I suggest above, the obvious authority would be a magistrate seeing that we are dealing with legal questions. Perhaps annual lists of blocks from each agency would be a good idea, with simply a number where secrecy has been approved. And the number of applications not approved would also be a significant check on whether magistrates were acting as rubber stamps.

A particular concern would be to ensure that in the case of (ca) requests dealing with criminal law in a foreign country, that the alleged crime in the foreign country is also a crime if it were committed in Australia.

While some may suggest that there should be a special authority to approve or oversee these requests, it seems to me that in view of the ineffectiveness of any block, that this is unnecessarily adding to the cost of the system. It also would suggest that a very large number of requests was envisioned!

A further appropriate measure to ensure accountability would be to include in the legislation provision for payment to individuals and organisations sustaining financial loss from disruptions that have

been caused by blockages where the activity of the individual or organisation is not in fact illegal. This would serve as a check on over-enthusiastic use of the mechanism.

I do not think that there is any question that the most appropriate way of implementing this proposal is to do so by legislation. The existing legislation clearly did not envision its use to block websites – I venture to say that in 1997 there would have been few, if any, members of parliament who had any real concept of what a web page really was. Although the start date of the World Wide Web (and hence web pages) can be set in 1993 with the introduction of Mosaic, in 1998 only 16% of Australians had internet access, and broadband did not really exist in Australia, so websites as we think of them today hardly existed.

Although I am not a lawyer, I would be astounded if the current use of s313 would stand up in court.

Respectfully submitted,

John I Denham

Background on J.I.Denham

I am a retired geophysicist, although I still am a member of the committee of the ASEG Research Foundation. For six years I was editor of Exploration Geophysics, a major scientific journal, and prior to this worked for 22 years for BHP Petroleum, where I was for some time Chief Geophysicist, and involved in the company's operations worldwide. Before that I was engaged in field geophysics in Australia and PNG, following graduation from Sydney.

Having first become directly involved with computers in 1973, and leading BHP Petroleum into the forefront of exploration computer technology, I have been an active internet user since 1997, and have made earlier submissions to inquiries on various telecommunications subjects.