Submission to

House of Representatives Standing Committee on Infrastructure and Communications

regarding

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

Executive Summary

Section 313 should be repealed in its entirety. It is currently quite unspecific and quite wide. It provides no certainty to carriers or carriage service providers as to what they can and cannot be asked to do. It permits such a wide interpretation of its purpose that it is bound to be misused by government, and used in ways that the original legislators did not intend.

General Comments on the Terms of Reference

The Committee ought to be reviewing s313(1) also i.e. not only s313(3).

The Committee ought to be reviewing all uses of s313(3), not only uses that aim to disrupt *potentially* illegal online services.

Section 313, as it forms the basis of Australia's de facto internet censorship regime, is important enough to warrant a full public airing. The Gillard government chose not to introduce specific legislation that would have set some boundaries on government activity in this area and instead chose to commence using Section 313 for this purpose. This avoided any public or parliamentary debate and scrutiny.

As is typical of government rhetoric on internet censorship, the Terms of Reference immediately jump in to talking about images of child sexual abuse. This is offensive to the intelligence of the reader as even the most cursory reading of s313(3) reveals that it can be used for so much more. There is a yawning chasm between “protecting the public revenue” (which might for example involve blocking access to the iTunes web site because Apple refuses to collect GST on behalf of the government -or- involve “checking up on” welfare cheats) and the INTERPOL “worst of” list. Along the spectrum from the one to the other, one might find “laws imposing pecuniary penalties” and “enforcing the criminal law” (generally).

The Terms of Reference do not make clear whether the government will contemplate amending s313 except regarding item (d) (transparency and accountability).

General Comments on Section 313

Extra-judicial action

One of the problems with s313 is that inevitably the government will be directing an ISP to block access etc. where the government has not shown that such access involves activity that *is* illegal, only that the government believes that it is *potentially illegal*.

This sets a bad precedent and establishes a regime where the government can effectively punish without recourse to the court. It establishes a regime where the government is judge and jury and the ISP is, perhaps unwillingly, executioner.

This is not how democracies are supposed to operate. If the government believes that something is illegal then it should be obliged to satisfy a court of this. This is how *some* (but unfortunately not all) of s313(1) operates, where, for example, a warrant from a court or the AAT is required in order to direct a telco to enable interception of a customer's phone line.

Limits of reasonableness

The test in s313(3), apart from the set of very broad categories of government interest, is “such help as is reasonably necessary”. As far as I am aware, this has never been interpreted by a court.

How far can the government go before something is deemed to be beyond “reasonable”? I don't want to find out the hard way as, for example, the people of the US and of the world are finding out about the activities of the NSA.

Is it “reasonable” because it is reasonable for the government to want to do something or is it “reasonable” because it is reasonable to expect an ISP to do something? This is not clear to me but I think the intention is the former i.e. ISPs can be asked to do things that they cannot reasonably be expected to do.

One of the problems is that an ISP may be unwilling to spend the time and/or money to test a

government request in court, or may choose not to test the validity of the request in court for other reasons. An ISP may therefore do something for the government that the government cannot validly ask it to do. C/CSPs are not appropriate guardians of human rights, nor should they be expected to fulfil this role.

It may or may not be in the interests of the ISP to carry out the request but it is often not in the interests of the customer for the ISP to carry out the request. As long as the customer does not find out, any conflict between the interests of the ISP and the interests of the customer does not cause a problem. Hence secrecy becomes an important aspect in getting ISPs to go beyond what is valid, but secrecy of government action is rarely a good idea.

It is a sad state of affairs when our human rights are only protected by ISPs and only in secret and only when it doesn't conflict with their own interests and only some ISPs, some of the time.

Legislators intention

If the government believes that a specific person has committed or is about to commit a specific crime then I think most people accept the idea that the authorities would target that person specifically and seek appropriate assistance from carriers/CSPs in doing so. However the use to which s313 is now being put goes beyond that to non-specific targeting of the entire population in case someone *might* commit a crime. That is in essence what blocking access to content is where potentially noone is Australia has even accessed the content.

Is that truly what the legislators intended?

s313 is a good illustration of the dangers of poorly written legislation containing weakly-constrained powers. Whoever voted for it should have his or her fat parliamentary pension revoked immediately.

s313 as it is now being used can only serve to undermine public confidence in the internet, in the same way that the NSA revelations have done. There are enough problems on the internet (for example, intermittent errors) without government being part of the problem.

Alternatives to s313

The government is wilfully and irresponsibly ignoring alternatives to the use of s313.

For INTERPOL “worst of” list entries the best option is takedown. It is completely effective. It is also generally quick, as any legitimate web hosting service would take down the content without the need for legal action or inter-government cooperation.

For sites involved in scams of various types (e.g. phishing, malware distribution) and for sites involved in other dubious activities (e.g. botnet, DDoS) the government should use a combination of takedown and notification to “warning” services that users can voluntarily subscribe to.

For example, my web browser automatically warns me if I visit a known “forgery” site. However it can only do that if someone has reported that site so that the site gets recorded in the list of known dodgy sites and then made available to my web browser. This is an option that I have voluntarily enabled in my web browser and I could disable it or override it if the government has made a mistake. That luxury would not be available to me if blocking is implemented by ISPs, as we saw with the ASIC / Melbourne Free University / 250,000 web site collateral damage debacle.

Political censorship

The recent wide-ranging and long-lasting, secret suppression order sought by the government and issued by Victoria's Supreme Court illustrates where we are going. If an internet censorship regime were not in place then people can laugh, shake their heads in bemusement, and read all about it on any number of foreign web sites. If an internet censorship regime were in place and in widespread use by government, we can only assume that all those foreign web sites could be blocked.

As many commentators have already observed, mere embarrassment for us or for our neighbours is no justification for censorship. The truth may be uncomfortable but that is a very bad reason to suppress it.

The fact that “national security” was cited as one justification for this secret suppression order just shows how abused and tired this excuse is getting. However we can see that government has not tired of using it and s313 is just the tool to get the most out of it.

When not using “national security” as the excuse I can imagine the government citing “operational reasons” for suppressing something or other.

Why should *anyone* trust that the government will not rapidly ramp up censorship beyond the INTERPOL “worst of” list, through the relatively trivial, all the way to political censorship?

As an aside, this case (the secret suppression order) really illustrates that government, not the people, needs to adapt to the changing world. The government is still trying to make the old rules work. We need new rules.

1984

The essence of s313 is a message to all carriers and carriage service providers that “you work for the government”. This is coupled with obsessive secrecy about what is being done. What better way to hurry us down the road to 1984?

Specific responses to the Terms of Reference

Which government agencies

With the disclaimer that I believe that s313 should be discarded, I see no particular reason to

restrict its use to certain government agencies, particularly given the vastness of the scope of s313. Almost any government agency can make a case for including itself within the scope of s313.

In the absence of an amendment to s313 it will always be valid for just about any government agency to get on the bandwagon. An agency can voluntarily *not* issue directions under s313 but equally the agency could change its mind at any time in the future, and do so without public debate.

Restricting the use of s313 to certain government agencies could lead to the situation where "unprivileged" agencies simply refer their requests to "privileged" agencies. This could cause all sorts of issues including but not limited to:

- the privileged agency has less expertise to assess the situation than the unprivileged agency
- the privileged agency gets bogged down in cases that it is not intended to or resourced to deal with
- action using s313 becomes more bureaucratic, more costly and less timely

Level of authority

With the disclaimer that I believe that s313 should be discarded, I believe that a warrant from an actual court should be required for *all* directions that the government gives to a carrier or carriage service provider under s313.

That would require the government agency to identify specifically what law it believes is being broken and to provide at least an outline of the evidence for its assertion. The court would then decide on the validity of the direction under s313 and effectively the court, not the government, would issue the direction. These checks and balances would require amendment to s313 in order to make them mandatory.

In *most* cases the victim of the direction or, failing that, some kind of public interest advocate should be permitted to argue in court as to why the direction should *not* be issued. In other words, for example, content on the internet should have its day in court before being blocked.

Obviously I exclude here, for example, that a victim would have a chance to argue against an intercept being put in place. s313 is barely needed for interception anyway as the details of how interception and access are authorised and executed are in another Act anyway. This is one reason why I am suggesting that s313 should be discarded.

Perhaps the intent of this question was regarding the level of authority within the agency itself. With the checks and balances proposed here, that question would become less important.

A requirement to satisfy a court about the illegality of the "service" raises questions about the validity of s313(3)(ca) however, because the then government ignored representations that any assistance to a foreign country should have a requirement for dual criminality. As it stands today, if

something is against the law of the foreign country, but not against the law of Australia a request for assistance could still be approved by the government and an ISP could then still be validly obliged to cooperate.

A requirement for dual criminality should be added to s313(3)(ca). It can be argued that the Attorney General would not approve assistance in the scenario set out in the previous paragraph but it cannot be argued that the AG would never approve such assistance and if such an argument were compelling then the requirement for dual criminality would have been in the legislation in the first place.

Characteristics of potentially illegal online services

I believe that s313 should be discarded. No content or service should be the subject of a blocking direction to an ISP.

If the content or service is illegal to host in the country in which it is hosted then mutual assistance should be used to get the country of hosting to have the content or service taken down. If the content or service is not illegal to host in the hosting country then the Australian government has no business with it.

If an activity is legal in Country X but illegal in Australia and I travel to Country X to carry out that activity then the Australian government has no business interfering in this, let alone attempting to prosecute me for doing so (although I am well aware that Australian governments have already passed legislation that is not in accordance with this principle). This is of course talking about something that happens in the real world. In the cyber world, you can imagine that my virtual self is travelling to Country X. The Australian government has no business interfering in this.

In the unlikely event that the Committee accepted this line of argument, it would not have any impact on the INTERPOL list, which lists content that is illegal to host everywhere.

In the more plausible scenario that the Committee does not accept this line of argument, then I would advocate that the characteristics be drawn as absolutely narrowly as possible.

The number of categories of content should be as few as possible. Each category should be defined precisely and narrowly. There should be an obligation on government to show that it is *actually* illegal, not just potentially illegal, with an appropriate “right of reply” from affected parties. For example, in the extreme, and assuming that the Committee does not see the folly of using s313 to block access to content, the Committee could settle on “the INTERPOL list” and nothing more.

However noone could sleep easily even with this arrangement because as sure as night follows day, new categories will be added later on and existing categories will be broadened. This has already been the experience overseas. Government has never even attempted to indicate how such “scope creep” will be *prevented*.

In addition, since we have already seen that government is fairly clumsy in its blocking attempts, with vast amounts of collateral damage, any given blocking request must be defined as narrowly as possible. That means, for example, if a web image is to be blocked, that image should be identified and the direction should concern that image alone. The government should not seek to block a whole web page unless the content (the text) of the page itself is illegal. The government should never seek to block an entire domain, let alone an IP address.

However some of this is somewhat specific to web content. Other types of access are likely to present even greater challenges and present an ever greater risk of collateral damage. For example, if the government discovered that illegal content was being distributed by email, would the government direct ISPs to examine all email as it passed through their servers, *a massive invasion of privacy*, and if the perpetrators responded to that by encrypting their email, would the government direct ISPs to block all email or to block all encrypted email?

Blocking is a fairly unhelpful approach to potentially illegal content. Government should not respond to failure to achieve effective blocking by becoming ever more clumsy and ever more heavy-handed.

Transparency and Accountability

With the disclaimer that I believe that s313 should be discarded, transparency and accountability measures should be *strong* and *mandatory*.

Transparency and accountability would be somewhat achieved by the requirement that all directions under s313 would have to be approved by a court.

In addition, I suggest that *all* such directions be individually published on a web site (run by an agency somewhat independent of government). ISPs would use this web site to get their directions just as the public would use this web site to ensure that s313 is not being misused (more than this very use is a misuse).

The web site would document:

- what agency sought the direction
- the date the agency sought the direction
- the general type of the direction e.g. block access to web image
- the date the direction was issued
- the entity to whom the direction was issued e.g. one specific C/CSP or all C/CSPs
- the specific law (act, section, clause etc.) that is alleged to be being broken

- the target of the direction e.g. URL to be blocked

- the status of the direction – statuses might include PENDING (court approval has been sought but not yet granted), ACTIVE (C/CSPs must act on the direction if any only if the status is ACTIVE), REJECTED (in the event that the court failed to approve the agency's request) and REVOKED (was ACTIVE but the agency no longer needs it). Note therefore that obsolete requests are maintained on the web site indefinitely as part of the transparency measures.

That way everyone, including other carriers/CSPs, can see exactly what directions the government is issuing. The only exception to this that I would allow is that if the URL is that of Child Pornography (as defined in Australian criminal law) then the URL need not be published and would not be published. It would be seen only by the target C/CSP(s).

The information on the web site must be available for download as a CSV file, in addition to the web page.

There must be a process to review whether any ACTIVE directions are still appropriate. In the case of Child Porn, where the URL would not be publicly visible, the responsibility to do that would rest with the original agency. For all other cases, the primary responsibility still rests with the original agency but review could be requested by any other agency or by the public.

It is critical that any blocking takes the form of a clear message that the content has been blocked, rather than behaviour that is not readily distinguishable from a legitimate error. The content of the block page can link directly back to the entry on the page of published blocking directions that is discussed above. The HTTP error code 451 has been rather darkly set aside for the purposes of indicating that the content has been censored.

I believe that transparency and accountability measures *must be* in legislation. This is the best that we can do (short of a constitutional amendment) to ensure that the measures are not quietly watered down later on. This will ensure that the measures are debated in the parliament and in public.

It should be noted that the Rudd/Gillard government already took submissions regarding transparency and accountability measures that would have been part of *their* internet censorship legislation, had that ever seen the light of day.

I think that documentation may have been on the old DBCDE web site but the present government seems to have buggered that up. The consultation (“Measures to increase accountability and transparency for Refused Classification material”) shows up in the search but the link gives a “not found” error. Most of it can probably be retrieved from the internet archive. Here is a link that may work for the final report from the public consultation.

https://web.archive.org/web/*/http://www.dbcde.gov.au/__data/assets/pdf_file/0020/129035/Outcome_of_public_consultation_on_measures_to_increase_accountability_and_transparency_for_refused_classification_material-web_version.pdf

However you really need to find the home page for that consultation in order to review the individual submissions.