Inquiry into the use of subsection 313(3) of the *Telecommunications Act 1997*

Submission by the Australian Communications Consumer Action Network to the Standing Committee on Infrastructure and Communications

August 2014

Australian Communications Consumer Action Network (ACCAN)
Australia's peak telecommunications consumer advocacy organisation
Suite 4.02, 55 Mountain St, Ultimo NSW 2007
Tel: (02) 9288 4000 | TTY: (02) 9281 5322 | Fax: (02) 9288 4019
www.accan.org.au | info@accan.org.au | twitter: @ACCAN_AU

About ACCAN

The Australian Communications Consumer Action Network (ACCAN) is the peak body that represents all consumers on communications issues including telecommunications, broadband and emerging new services. ACCAN provides a strong unified voice to industry and government as consumers work towards availability, accessibility and affordability of communications services for all Australians.

Consumers need ACCAN to promote better consumer protection outcomes ensuring speedy responses to complaints and issues. ACCAN aims to empower consumers so that they are well informed and can make good choices about products and services. As a peak body, ACCAN will represent the views of its broad and diverse membership base to policy makers, government and industry to get better outcomes for all communications consumers.

Contact

Xavier O'Halloran
ACCAN Policy Officer

Suite 402, Level 4
55 Mountain Street
Ultimo NSW, 2007
Email: info@accan.org.au
Phone: (02) 9288 4000
Fax: (02) 9288 4019
TTY: 9281 5322

Table of Contents

Introduction

The Australian Communications Consumer Action Network (ACCAN) is supportive of efforts to prevent illegal activity online. Consumers are vulnerable to a number of illegal activities such as online scams. Without active regulators consumers are likely to lose confidence in transacting online. As with all exercises of executive power, there must be a consideration of proportionality, transparency and accountability. The current operation of Section 313(3) of the *Telecommunications Act* will be analysed on these three grounds. ACCAN's submission will highlight the negative impact this section can have on consumers and small business when it exceeds its intended scope and explore possible ways to make it fit for purpose. Small business website owners are particularly vulnerable to this type of law because of its potential for misapplication and the costly nature of appeal.

Is there a need for protection?

As the Terms of Reference point out, Section 313 has been used by the Australian Federal Police to authorise Internet Service Providers (ISPs) to block the INTERPOL 'Worst of' child abuse list. As INTERPOL recognises, the Web is the most accessible and visible means to access child exploitation material despite not being the most important, in terms of numbers of files.[1] As such, blocking access to these websites is an important step police and industry can take to prevent crimes against children from continuing undisturbed.

The INTERPOL 'Worst of' child abuse list is a useful example of both the need for protection and a process for administering a list of blocked material. Unlike Section 313 the INTERPOL list has some measures to ensure it remains proportionate, transparent and accountable. This will be discussed in detail below.

The other example listed in the Terms of Reference is the prevention of online services in breach or potentially in breach of Australian law, for example financial fraud. In 2013 online scams caused more financial harm than any other delivery method. The reported cost to Australians was close to $42 million.[2][3] Phishing and identity theft scams often rely on directing consumers to fake websites which appear to be well-known government, corporate or financial entities. Consumers are persuaded to hand over account details, such as usernames and passwords, which scammers then use for personal gain. Educating consumers to be wary online and prosecuting offenders are the most important steps in stopping this crime. However, the ability to directly block these websites may be necessary in order to halt the fraud during the investigation phase.

It is unclear at this stage if website blocking is being used merely during the investigation stage. In some cases it appears this power is being used by government authorities as a permanent solution rather than a short term measure to prevent ongoing crime until prosecution takes place. Given the accessibility and visibility of websites, there may be cases that a law directed at blocking access in a timely way to potentially illegal material may be necessary. However the current law goes too far and is ill equipped for this purpose.

---

[1] http://www.interpol.int/Crime-areas/Crimes-against-children/Access-blocking/The-INTERPOL-%22Worst-of%22-list

[2] ACCC, 2014, 'Targeting scams – Report of the ACCC on scams activity 2013', June 2014, available at: http://www.accc.gov.au/system/files/Targeting%20Scams%202013.pdf

[3] This figure only includes scams reported to the ACCC. The actual figure is believed to be much higher.

Problems with Section 313(3)

Section 313(3) is a 'catch all' provision designed to authorise telecommunications providers to give officers and authorities of the Commonwealth and of the States and Territories "help as is reasonably necessary" to, among other things, enforce criminal law and laws imposing pecuniary penalties. As it is currently applied this is a fairly low threshold. It requires no judicial assessment of the evidence and places a large burden on internet service providers in determining what "help is reasonably necessary". There are also no tight controls on the types of government authorities empowered to use this Section. As a result it potentially allows government agencies, such as local authorities like the Gundagai Shire the power to request ISPs shut down web services.

Outsourcing enforcement to ISPs

Some ISPs may use this power judiciously. For example, iiNet's Steve Dalby stated in relation to the ASIC requests made public under freedom of information:

"There's no way we'd block websites on the strength of 'pursuant to investigations' for 'possible contraventions'. Not only that, but there seems to be no senior authorisation, just a middle manager signing off."[4]

While iiNet may be a responsible actor in this field, a scheme which relies on ISPs keeping government accountable is not ideal and is likely to give little comfort to citizens in a democracy.

Scope of offences covered by the law

Another problem is the scope of the term "criminal law and laws imposing pecuniary penalty". The law is open to the possibility of perverse outcomes, such as suspending a consumer's internet connection to help secure payment of a parking fine. However it is not necessary to think up worst case examples, we need only look to how the law has been applied in recent history.

In 2006 the Prime Minister's office allegedly used the power to shut down a parody of John Howard's website operated by writer Richard Neville.[5] The site contained a speech 'apologising' for the Iraq war. According to the domain name registrar, Melbourne IT, the website was shut down on copyright infringement grounds and that it "look[ed] like a phishing site".[6] Leaving aside the merits of this case, it is clear that allowing service providers and government authorities to interpret complex legal issues invites trouble. For example, such an application has the potential to undermine the rule of law, the constitutionally implied freedom of political communication and the since enacted fair dealing copyright exemptions for parody and satire. It is unreasonable for an ISP or indeed most government authorities to be the arbiters of these legal issues without judicial intervention.

Part of the problem is allowing such an expansive power to be used in relation to relatively minor offences, such as claims of copyright infringement. The act of shutting down a web service and impacting a legitimate business is rarely going to be proportionate to an offence which merely attracts pecuniary penalties. A failure to adequately confine s313 to 'serious offences' can have a

[4] http://www.zdnet.com/au/iinet-slams-asics-ip-blocking-notices-7000017519/

[5] http://www.smh.com.au/news/breaking/government-shuts-howard-spoof-site/2006/03/17/1142098638843.html

[6] http://www.smh.com.au/news/breaking/government-shuts-howard-spoof-site/2006/03/17/1142098638843.html

number of unintended consequences and lead to decisions which are out of proportion with the harm being caused.

Misapplication of the law

The broadness of the law potentially invites misapplication. For example, not confining the law to use by government authorities with particular experience in internet based crime is cause for concern. In 2013 it was revealed ASIC had accidently ordered the blocking of access to 1,200 websites which shared the same IP address as an offending website.[7] IP addresses are a finite resource and sharing across multiple websites is not unusual. This should have been known to a law enforcement agency specialising in internet based crime. Currently the power can be used by a variety of government authorities, such as local councils, who are likely to have limited technical expertise.

Impact on website owners/small businesses

As the ASIC example shows this misapplication of the law can be particularly detrimental to small business website owners. One of the sites caught up in this mistake was the Melbourne Free University (MFU), an academic-run community organisation which hosts free public lectures.[8] The website was inaccessible for nine days after an unknown government authority ordered the IP address linked to the site be blocked. It subsequently took six weeks of investigation by journalists and Electronic Frontiers Australia to discover ASIC was behind the block.

In many respects the Melbourne Free University was well placed to draw attention to the mistake and subsequently have the block lifted. As the site owners said:

"We have to wonder, if we weren't the sort of organisation that we are, whether we would have been able to raise this level of concern about our site being blocked, and whether anything would have been done. What if we were a small business or a lone individual?"[9]

As a small business consumer representative body ACCAN is particularly concerned that not all website owners would have the same ability to draw attention to a block. As the law is currently being applied, site owners are unlikely to know the reasons behind the block or any avenues for appeal.

The impact of such a block on small business is likely to be extremely costly to both reputation and/or direct loss of sales. ACCAN-commissioned research found that 66% of small businesses would find even one day without fixed broadband services to be severe or catastrophic to their business.[10] Similarly a website block lasting nine days, as MFU experienced, would likely be highly damaging to a small business, especially those using websites to conduct e-commerce.

It should be noted that the power goes beyond simply shutting down websites. By targeting IP addresses government agencies could also inadvertently be shutting down other services, such as

---

[7] http://www.abc.net.au/news/2013-05-16/westendorf-and-atahan---internet-filter/4694252

[8] http://www.abc.net.au/news/2013-05-16/westendorf-and-atahan---internet-filter/4694252

[9] http://www.abc.net.au/news/2013-05-16/westendorf-and-atahan---internet-filter/4694252

[10] Market Clarity, 2013, 'Small business Telecom Service Use', available at: https://accan.org.au/files/Market-Clarity-Small-Biz-Telecom-Service-Use-final.pdf p.58

cloud operating platforms. Government is encouraging small business to embrace more efficient methods of operating, such as cloud computing.[11] The 'cloud' can be used to operate almost every internal and external business process, so inadvertently shutting down these web services would potentially be crippling to business.

Ensuring proportionality, transparency and accountability

Turning to the questions the Committee is 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.

One way to confine the number of government agencies with access to the provision is to limit the use of the power to 'serious criminal offences'. In turn limit access to only those agencies empowered to enforce 'serious criminal offences'. Definitions of a 'serious criminal offence' differ in each jurisdiction, so a definition may need to be developed, perhaps linked to the maximum penalty units for an offence.

As mentioned already there are particular problems in allowing authorities without online law enforcement expertise to exercise these powers. Part of any solution should include accreditation for agencies and/or officers empowered under this law, to ensure they receive adequate training in law enforcement related to 'online services'.

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

These requests should be accompanied by a court order and other protections outlined in this submission. Government agencies should only be using these powers without judicial oversight in special circumstances. As stated there may be occasions where a quick, ongoing response is required to combat offences from being perpetuated online. If an agency is making a request it should only be made by senior officers with reasonable grounds. To improve accountability the number and scope of these requests made by an agency should be reported annually.

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

It should be understood that the exercise of this power represents, in some cases, a significant curbing of individual rights, without judicial scrutiny. Such a power needs to be balanced to ensure the power is exercised in proportion to the nature of the offence. This is implicit in the INTERPOL 'worst of' list which is targeted at child exploitation material. For example, offences related to dissemination and possession of child abuse material in all Australian jurisdictions is classed as 'serious criminal offences'. Confining this power to serious offences ensures proportionality is embedded in any decision to target web services.

11 http://www.minister.communications.gov.au/malcolm_turnbull/news/new_tools_to_help_small_businesses_adopt_cloud#.U9r_neOSwrU

(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.

The criterion for inclusion in the INTERPOL "Wost of" list includes a number of transparency and accountability measures. Firstly, multiple agencies must verify that the websites contain material meeting the INTERPOL definition of child sexual abuse material. Secondly, the INTERPOL scheme contains a 'stop page' which states the site has been blocked, names the agency that has enforced the block and links to an appeal mechanism.[12] These measures should be a bare minimum. Without them website owners are unlikely to know why their website is blocked, let alone what rights to appeal they may have.

If the power is mistakenly applied the impact on small businesses and other website operators could be minimised by having a quick, accessible and free path for appeal. There are already established review mechanisms for these types of administrative decisions. In cases of mistake, reconsideration by the original decision-maker is likely to solve the problem in a timely manner, without the need to seek judicial review.

As mentioned above, greater transparency and accountability in individual cases should be accompanied by annual public reporting by government agencies using this power. This should help ensure the power is being applied appropriately.

Conclusion

ACCAN would like to thank the Standing Committee for the opportunity to contribute to this consultation. We see a need for this type of power on consumer protection grounds in relation to serious criminal offences. However, we remain concerned that the power, as currently drafted, is too broad. A greater role for judicial oversight, only using the power in relation to serious criminal offences and greater transparency around methods of appeal will allay many of the concerns related to this power. Without these measures there is potential for many consumers, especially small businesses and website owners to suffer financial and reputational damage. For small businesses the expense of legal counsel coupled with the exemption from liability this section gives providers and government agencies means these costs may never be recouped.

As with all exercises of executive power this section should be grounded in a consideration of the proportionality, transparency and accountability of the law.

[12] http://www.interpol.int/Crime-areas/Crimes-against-children/Access-blocking/Complaints-procedure