Internet Society of Australia
A Chapter of the Internet Society
ABN 36 076 406 801

PO Box 1705
North Sydney NSW 2059

25th August 2014

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

1. Introduction

The Internet Society of Australia (ISOC-AU) welcomes this inquiry and the opportunity to provide a submission. In 2013, when ASIC's use of Section 313 (the Section) of the Telecommunications Act 1997 (the Act) to block websites came to light, ISOC-AU, along with many other civil society, industry and consumer groups expressed concern about the lack of process, accountability and oversight that these incidents revealed.

ISOC-AU believes that while the intent of the section *could* be preserved, a framework for its use is urgently required recognising the public interest and ensuring legitimacy, openness, transparency and accountability. Without such a framework the section should be removed.

ISOC-AU believes that this provision in the Act should only be used in cases of extreme harm, and with clear evidence that a serious crime will take place, or is taking place, unless such measures are taken.

In the limited cases where the use of the Section may be warranted, there should be a process that ensures that only the identified site(s) and service(s) are blocked. For example, where the intent is to prevent access to a website, the request should specify that only http/s traffic to a particular domain name should be affected.

In cases where site or service blocking is merited, blocked sites should be redirected to a holding page indicating the organisation that has requested the

block, providing contact details for that organisation and specifying process for appealing the block.

Further use of the Section to impede or cause the cessation of broader communications services must only be instituted when extreme circumstances "safeguarding national security" are the case. These actions must also be necessary and proportionate to the act in progress.

2. Agencies Which Should Be Permitted To Make Requests

In order to ensure that the use of s313 to disrupt online services is conducted in a technically competent manner, and that such uses are subject to appropriate oversight, the list of agencies permitted to make such requests should be kept as small as possible.

This list should be no larger than those agencies that are currently able to request surveillance warrants, and such requests should be centrally managed through a single agency, such as the ACMA of the Attorney-General's Department.

3. Level of Authority Required

Access to the Internet is essential for participation in the modern Australian society. Any action by carriers or carriage service providers (Providers) that could interfere with a person's use of the Internet, therefore, should only be taken when there is a demonstrable threat of serious criminal activity. There must also be transparency and accountability for any such actions taken by a carrier or carriage service provider.

Nature of the Offences Covered

The circumstances in which law enforcement officers and authorities (Commonwealth, State or Territory) can require assistance from Providers are widely drawn – ranging from criminal law to laws that impose 'pecuniary penalties'. Because such assistance involves an individual or organisation's access to the Internet, it should only be requested when the serious harm is threatened or committed. The current wording of the Act is such that it could conceivably be applied today to trivial misdemeanours that happen to carry a fine, no matter how minor.

Use of the Section should therefore be confined to criminal laws where the offence attracts a maximum penalty of at least two years imprisonment for an individual.

Probability of the Offence Being Committed

Nothing in the Section requires that the relevant officer or authority have some minimum level of belief that the offence is likely to be or have been committed. ISOC-AU believes that it should be required, at the barest minimum, that a 'senior officer' of a police force, or judicial officer, have 'reasonable grounds' for a belief in the likelihood of a serious crime will be (or has been) committed before any request under the Section is processed.

4. Online Services Which Should Be Subject To Requests

ASIC's previous use of the Section demonstrates the technical complexity – and limitations – of blocking websites. Because in these instances the IP address was selected for blocking, and the target website(s) were hosted on shared servers, it resulted in over 250,000 'innocent' websites being blocked.

In this situation had the server in question also been running email, telephony, or conferencing services for example, these also would have been blocked. This indicates the scope applies to all forms of communications, not merely words, but services.

While ISOC-AU acknowledges that blocking known criminal websites may have limited value, it has consistently argued against blocking websites more generally because it is neither practical nor effective. It does not prevent access to a vast array of criminal material on the Internet either because it is delivered by means other than the web or because the URL of the material varies with each access.

It is understood that the most likely basis for a request under the Section is to prevent access from Australian networks to particular websites. There may also be circumstances where preventing access to other services, such as File Transfer Protocol (FTP) or email may be merited.

Further use of the Section to impede or cause the cessation of broader communications services must only be instituted when extreme circumstances "safeguarding national security" are the case. These actions must also be necessary and proportionate to the act in progress.

5. Transparency and Accountability

A framework of transparency and effective accountability is critical to ensure that the public interest is protected, and use of the Section is kept to the absolute minimum. ISOC-AU recommends the following mechanisms be written in to the Act to achieve such a framework.

Redirected blocked websites

As noted above, in cases where site or service blocking is merited, blocked sites should be redirected to a holding page indicating the organisation that has requested the block, providing contact details for that organisation and specifying process for appealing the block.

Appeals

There are two situations under the Act where there should be an avenue of appeal.

The first is for parties injured by actions taken by a Provider under the Section that have wrongly injured the person, or organisation, the subject of a Section action. Under that Section, the Provider is not liable for actions they undertook under that section 'in good faith'. However, there should be a mechanism that can test both whether the relevant authority or agency had reasonable grounds for requesting the Provider actions, and whether the Provider was, in fact, acting in good faith.

ISOC-AU therefore recommends that appeals be allowed by a federal court under Chapter 3 of the Constitution (either or both the Federal Court of Australia and the Federal Circuit Court) for actions taken under the Section, testing whether the authority or agency had reasonable grounds for requesting Provider action and whether the Provider acted 'in good faith' in implementing the Section request. This court should therefore be given a specific statutory power to order either the requesting agency/officer and/or the implementing Provider to pay compensation to harmed innocent third parties, if the actions were carried out in bad faith or recklessly (ie a higher bar than negligence).

Section 314 provides for arbitration in situations where the Provider does not agree with the terms and conditions under which they are required to comply with a Section request. In that arbitration, the arbitrator must be a specified person, (or class of persons) as determined by the Minister. Regulations can also provide for the conduct of such arbitration.

ISOC-AU therefore recommends that the Minister, after public consultation, determine a framework for the appointment of qualified arbitrators and arbitration processes that will be fair and accessible to all parties.

Rectification and Resumption of Service

Cases may occur where a system has been exploited by a third party that has led to the criminal activity. This may occur where, for example, a computer system has been compromised and extreme material, or services to divert legitimate

systems, have been established on the system itself. In this case a site or system operator should be able to rapidly remove the criminal elements of the system and restore legitimate operations. In this case network services should also be restored rapidly.

ISOC-AU therefore recommends that any mechanisms established include the right for rapid restoral of normal operation of legitimate systems.

Cost Recovery and Appeals

Network operators should have reasonable cost recovery mechanisms in place for such a regime. Such a system has been able to be implemented successfully under the provisions in the Telecommunications Interception and Access Act. Furthermore, should costs be disputed an avenue must exist for appeal.

ISOC-AU therefore recommends that Network operators should have reasonable cost recovery mechanisms in place and an appropriate appeals mechanism should costs be disputed.

Reporting

A reporting regime, similar to that currently in place for the Telecommunications Interception and Access Act, is necessary to ensure transparency. Such reporting should list the number of requests per agency and should include the basis on which each request is made (e.g. the relevant offence). Such reporting should also include summary data on the number of requests made by ASIO.

About the Internet Society of Australia

The Internet Society of Australia (ISOC-AU) is a non-profit society founded in 1996 which promotes the Internet development in Australia for the whole community – private, academic and business users: the Internet is for everyone! ISOC-AU is a chapter of the worldwide Internet Society and is a peak body organisation, representing the interests of Internet users in this country. We have a longstanding and ongoing commitment to the effective representation of these interests in legislative and policy review, code development and self-regulatory processes in the telecommunications, domain name and Internet-related services industries.

George Fong
President
Internet Society of Australia