Electronic Frontiers AUSTRALIA
20 YEARS

PO Box 1302, Kensington VIC 3031
W www.efa.org.au T +61 3 9013 9492
E email@efa.org.au F +61 3 9013 9468
@efa_oz

Committee Secretary
House of Representatives Standing Committee on Infrastructure and Communications
Parliament House, Canberra ACT 2600

1st September 2014

Dear Committee Secretary,

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

EFA welcomes the opportunity to provide input into this review. Please find our submission on the following pages. Please do not hesitate to contact me should you require any further information.

About EFA

Celebrating its 20th anniversary in 2014, Electronic Frontiers Australia, Inc. (EFA) is a national, membership-based non-profit organisation representing Internet users concerned with on-line freedoms and rights.

EFA is independent of government and commerce, and is funded by membership subscriptions and donations from individuals and organisations with an altruistic interest in promoting online civil liberties. EFA members and supporters come from all parts of Australia and from diverse backgrounds.

Our major objectives are to protect and promote the civil liberties of users of digital communications systems (such as the Internet) and of those affected by their use and to educate the community at large about the social, political and civil liberties issues involved in the use of digital communications systems.

Yours sincerely,

Jon Lawrence
Executive Officer

Submission regarding 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

Introduction

Electronic Frontiers Australia (EFA) has prepared this submission to comment on the use of section 313 of the *Telecommunications Act 1997* (Cth) (s313) by government agencies to disrupt the operation of illegal online services. EFA seeks to promote digital consumers' rights and believes that these rights are not adequately represented with the excessive scope of s313.

EFA believes that s313 is a dangerous impediment to Internet freedoms. It was enacted with a strong consideration of the *Convention on Cybercrime* and subsequent *Cybercrime Legislation Amendment Bill 2011*. The purpose of s313 appears, on face value, to assist Law Enforcement and National Security Agencies (LENSAs) in their pursuit of the prevention and prosecution of offences under Australian law. Section 313 attempts to achieve this by legislating for maximum cooperation by carriers in disrupting any illegal activity from being performed over their infrastructure.

EFA asserts that, inter alia, s313 is superfluous in achieving these outcomes. In fact, EFA is of the position that s313, in its current form, is against the public interest. EFA recommends that s313 be struck out, or, in the alternative, its scope be restricted by a narrow definition. Should the latter be considered, EFA suggests that, without a specific scope of power and without a system of judicial checks and balances, this section will not be able to satisfy the public interest.

EFA would like to raise the following arguments to support its recommendation.

Implications for content filtering and censorship

The vague wording and broad scope of s313 has far-reaching potential for abuse. Section 313 has been used predominantly as a tool for blocking specific websites. In principle, EFA is opposed to the blocking of websites as such actions are relatively trivial to circumvent and possess an inherent risk to freedom of expression. EFA accepts however that there may be certain circumstances where blocking specific websites may be in the public interest, and that carriers play a crucial role in facilitating this. However, a degree of proportionality is necessary to avoid over-extending the powers under s313.

There are a number of examples where the use of s313 as a filtering tool has failed, with great cost to legitimate websites. The most well-known of these is the unintentional disruption of over 250,000 websites by ASIC in 2013[1]. This disruption was clearly the result of a lack of technical knowledge and demonstrates both the need for properly documented processes and the risk of very significant collateral damage from such actions. This is particularly true given the current lack of restriction on the use of s313 which is currently available to *all* government agencies.

[1] https://www.efa.org.au/2013/06/05/asic-blocked-250000-sites/

Electronic Frontiers AUSTRALIA 20 YEARS

Implications for Personal Privacy of Users

There are also a number of privacy implications for users that attempt to access blocked websites.

One concern is that of access to incoming traffic. For instance, when a website is 'taken down' at the request of a government body, a visitor to that website faces several privacy concerns - their visit is easily traceable, the user's IP address can be logged, and any attempts to dispute a take-down (usually by the host) would require them to reveal their identity.

Section 313 is particularly susceptible to mission creep. The broad wording of terms such as 'offence', 'do the carrier's best', and the wide range of 'purposes' means that almost any breach of any Australian law, even the trivial, would oblige an ISP to *actively* cooperate with government agencies. The implications for overreach are therefore self-evident. It can be used as a quasi-device for the collection of metadata, or as a means of achieving purposes that are otherwise unable to be achieved by other legislation (which had been put through far greater parliamentary scrutiny).

Unclear Processes

Section 313 in its present form suffers from a number of administrative and legal deficiencies. As mentioned above, the vagueness of the wording gives this provision enormous (and unclear) scope. It is also problematic that the concept of 'doing their best' has not been put through any judicial scrutiny, so that the limits of this term are uncertain and tend to err on the side of carrier proactivity.

Furthermore, there are no administrative restraints, processes or oversight to determine whether this provision is being misused by officials. The open wording makes the process of data disruption vulnerable to informal procedure. It also omits any system of checks and balances - which are often vital components of other similar powers in the *Telecommunications Act 1997* and the *Telecommunications (Interception and Access) Act 1979*.

Section 313 does not hold any disclosure or transparency requirements, unlike many other administrative instruments, such as warrants, data preservation notices or ACMA take-down requests. As such, it is impossible to ascertain what this power is being used for or how extensively it is being used.

For example, it is unclear whether s313 could be used to obtain a user's metadata or disrupt a user's connection. Such a request would inevitably assist in government operations, but at the cost of other more stringent administrative processes. Recent examples involving Telstra's cooperation with Commonwealth bodies[2] demonstrate that these concerns are very real.

In summary, s313, in its present form, is a significant potential threat to the public interest. It is vague, vulnerable to administrative over-reach, and is not subject to any established system of checks and balances. The potential for abuse is virtually unlimited. It offers broad powers with almost no restrictions. It is for these reasons that EFA recommends that s313 be struck out completely. If it is not struck out completely, the above issues need to be adequately addressed.

[2] http://www.zdnet.com/au/telstra-hands-over-browsing-history-in-current-warrantless-metadata-regime-7000032717/

Electronic Frontiers AUSTRALIA 20 YEARS

Addressing the Terms of Reference

A. Which government agencies should be permitted to make requests pursuant to s313 to disrupt online services potentially in breach of Australian law from providing these services to Australians?

EFA recommends that s313 be struck out completely. As such, there is no need for *any* government agencies to require the use of s313 as each respective agency has their own alternative means of achieving their respective outcomes.

Should s313 remain, EFA strongly recommends that the list of government agencies able to employ s313 be as limited as possible. This is to prevent administrative over-reach, and to ensure that each agency has the competence and technical knowledge to carry out its duties with minimal collateral damage. EFA believes that it would be appropriate to limit the permitted agencies to law enforcement and national security agencies, and to ensure that only the most serious offences are targeted. It would also be appropriate for all requests to be managed through a central agency, such as the Attorney-General's Department.

B. What level of authority should such agencies have in order to make such a request?

Recommendations

1. The agencies with the authority to make requests under s313 should be limited to LENSAs, for the enforcement and prevention of Australian criminal laws (and not those of foreign countries).
2. If the number of agencies is to be expanded beyond LENSAs, the authorised agencies should be limited to those that oversee serious breaches of Australian law, such as ASIC. Similar bodies, such as the ACCC or ACMA should not have access to s313, as they have existing measures in place to enforce their sphere of legislative power.
    a. The extension of authorised agencies beyond LENSAs is subject to the simultaneous revision of the threshold of the offence. For instance, if ASIC is authorised to submit requests under s313, a minimum threshold must be applied for the offence in question - such as a minimum civil penalty of 100 penalty units or a criminal offence carrying a minimum of 3 years imprisonment.
3. Remove s313 (3)(ca) and s313 (4)(ca) - a foreign body should not have access to such broad obligatory assistance from Australian ISPs, especially with no safeguards, as is the present case.
4. The entirety of s313 should be reworded to allow for a carrier's discretion to assist agencies. As s313 stands, carriers are obliged to comply with agency requests 'as best' as they can. This does not take into account the legitimacy of the claim or the authority of the agency. The wording ought to be revised to enable the carrier some means to have a request reviewed, if they believe that the requesting agency may be in error, or resorting to s313 when alternative measures would be more appropriate.

Electronic Frontiers Australia, Inc.
ABN 35 050 159 188
www.efa.org.au
Your voice for digital freedom, access and privacy since 1994

C. The characteristics of illegal or potentially illegal online services which should be subject to such requests

In its current form, s313 (3)-(4) cover a grossly excessive range of domestic and foreign matters. It currently covers all offences carrying a criminal or civil pecuniary penalty, including any criminal offence of a foreign country - whether it is also a domestic crime or not. The scope of s313 (3)-(4) also covers *any* matter of public revenue and any matter directly or incidentally related to the undefined 'national security'.

As it stands, s313 would compel carriers to cooperate with *any* Commonwealth or State body, in regard to almost *every* breach of Australian law, including criminal law of a foreign country. The existing threshold is dangerously broad, and creates immense obligations on carriers to cooperate with even the most minor of infringements.

Recommendations

1. Insert an express and clear minimum threshold on the nature of the offences covered. For instance, EFA recommends that s313 should only apply to breaches of Australian law that carry either a minimum criminal penalty of 3 years imprisonment, or 100 penalty units.
2. Insert provisions for a burden of proof on behalf of the requesting agency. This would require the agency to raise reasonable arguments to justify their request for assistance. Currently, there is no provision that takes into account the probability of the offence occurring, or even a provision linking the victim party to the offence itself.

D. What are the most appropriate transparency and accountability measures that should accompany such requests, taking into account the nature of the online services being dealt with, and what is the best/appropriate method for implementing such measures?

Currently, s313 has no system for checks and balances. There is no way for the Australian public to know what is being requested, how many requests are made, who is making requests or the extent of a carrier's compliance. The aforementioned Telstra example is one instance in which the Australian public were left in the dark as our largest ISP provided LENSAs with users' browsing history without a warrant.

Earlier, EFA had raised the example of ASIC's blocking of over 250,000 websites using s313, many of which were illegitimate collateral damage. Currently, the Australian public has no way of knowing what sites have been blocked, or what has been censored, until it is too late. For legislation obliging Australian carriers to 'do their best' to prevent almost *any* offence, there are no mandatory transparency or accountability measures. This significant gap between scope and accountability is a gaping hole in Australian law, and poses a very real threat to online civil rights and freedom of Internet users.

Electronic Frontiers Australia, Inc.
ABN 35 050 159 188
www.efa.org.au
Your voice for digital freedom, access and privacy since 1994

In addition, s313 carries very little, if any, judicial scrutiny. There is no common law relating to this section[3], and as such, no interpretation of the wording and scope of power therein. Most other areas of law have gone through the Courts and each pivotal term has been given its due diligence. Section 313 has not, and remains open to unlimited interpretation.

Accordingly, EFA reasserts that s313 be struck out. In the alternative, it should be subject to stringent administrative transparency and accountability measures.

Recommendations

EFA recommends, *inter alia*, the following:

1. The introduction of an adequate system of reporting, similar to those required of government agencies requesting access to communications data under the *Telecommunications (Interception and Access) Act 1979 (Cth)*.
2. The introduction of appeal provisions via the Administrative Appeals Tribunal or other Court. This would enable both owners of websites which are blocked and the carriers asked to perform the blocking to have the decision reviewed if they believe the powers are being misused.
3. Oversight by an independent agency with experience in technical enforcement, so inappropriate requests such as the ASIC incident can be queried before action. It would also be appropriate for the carrier to have a clear mechanism to query the technical appropriateness of requests. The latter syncs well with EFA's aforementioned recommendation for greater ISP discretion (rather than strict obligation to comply).

[3] http://www.austlii.edu.au/cgi-bin/sinosrch.cgi/au?method=boolean&rank=on&query=cth%20consol_act%20ta1997214%20s313