Why Australia Needs Site-Blocking

Sadaat Cheema argues that site-blocking would be an effective and proportionate measure to deal with online copyright infringement in Australia.

INTRODUCTION

With increasing access to high-speed internet and growth in the popularity of file-sharing software (such as BitTorrent), online copyright infringement continues to be a significant issue in many Western countries, Australia included.

Site-blocking does not remove, delete or alter infringing content. It targets the end-user rather than the originator of the content.

On 7 April 2015, the Dallas Buyers Club LLC succeeded in obtaining preliminary discovery of the identification details of approximately 4,726 internet subscribers, suspected of having infringed copyright in the 2012 Jean-Marc Vallee film, *Dallas Buyers Club*. This decision is the first of its kind and opens up the potential for rights-holders to take action against individual internet subscribers. The High Court of Australia has also previously noted, in *Roadshow Films Pty Ltd v iiNet Limited* [2012] HCA 16, that more than half of the usage of iiNet's internet services by customers was attributable to BitTorrent.[1] iiNet is Australia's second largest internet service provider (**ISP**).[2]

At the same time, legislators are turning their attention towards ISPs, as the link between high-speed internet and potential copyright infringement has not gone unnoticed. On 26 March 2015, the Australian Government introduced the *Copyright Infringement (Online Infringement) Bill* (the **Bill**) which amends the *Copyright Act 1968* (Cth) (**Copyright Act**) to enable copyright owners to apply for an injunction requiring ISPs to block access to overseas websites the primary purpose of which is to *'infringe … or facilitate an infringement of copyright'*. In determining whether to grant an injunction, the Court is required to consider a non-exhaustive list of factors including *'whether disabling access to the online location is a proportionate response'*. At the time of writing, the Bill has been presented and read for the first time in the House of Representatives.

The Government's proposal comes in the midst of a polarising debate over the effectiveness, proportionality and due process of a future site-blocking regime. While the entertainment industry regards site-blocking as '*uncontroversial*', the peak telecommunications industry body fears that it could result in unintentional blockage of legitimate websites.[3]

This article argues that site-blocking is, in principle, an effective and proportionate measure to deal with online copyright infringement. It suggests that while some criticisms of siteblocking are valid, they fail to appreciate the nuances of site-blocking, particularly the technical capabilities of the different site-blocking technologies that are available. Having said that, the Government's proposal falls short on important issues. It fails to ensure that a court will give due consideration to selecting a suitable technical measure and the Bill also fails to address a real risk that many applications for site-blocking will go unopposed. These are issues that need to be resolved.

WHAT IS SITE-BLOCKING?

Online copyright infringement can happen in a number of ways: *server-based* models, such as streaming and usenet; *peer-to-peer* networks, such as BitTorrent; and *cloud-based* models such as online locker services. Each model requires that end-users obtain access to a website to begin the download process.

ISPs exercise control over key elements of internet networks which are essential to website accessibility. When a user seeks access to a web page, they rely on a number of internet-related services to transmit data from their computer to the relevant website:

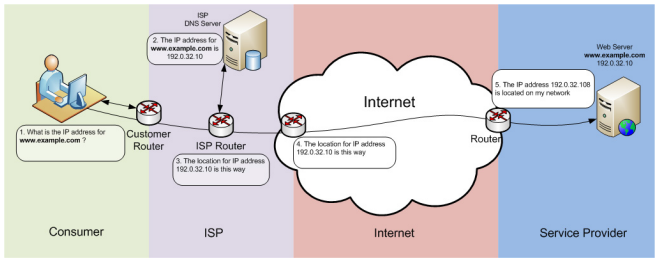
- internet connectivity, as supplied by the ISP;
- Domain Name System (**DNS**) server, which converts a domain name (www.example.com) into an IP address (an IP address is akin to a telephone number; it signifies a particular location (eg of a web server) on the internet);
- network routing, being hardware devices which direct data along the quickest route to an intended destination; and
- web servers, which host websites.[4]

1 *Roadshow Films Pty Ltd v iiNet Limited* [2012] HCA 16 [38].

2 ABC, 'Hollywood studios lose iiNet download case' <http://www.abc.net.au/news/2012-04-20/iinet-wins-download-case/3962442>.

3 Sydney Morning Herald, 'Online pirates hit choppy seas', <http://www.smh.com.au/federal-politics/political-news/online-pirates-hit-choppy-seas-20141212-125ief.html>.

The regulator of communications in the United Kingdom, **Ofcom**, has produced the following diagram to illustrate how data flows along the internet.

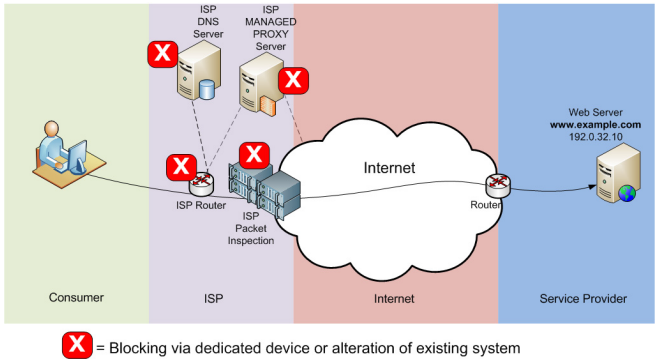


Source: Ofcom.[5]

There are four main technical measures that ISPs can adopt to manipulate the flow of data on the internet and effect a site-block:

- **Blocking by IP Address:** The ISP configures its routers so that data packets that are addressed to an infringing IP address are redirected away from the intended destination.[6]
- **Blocking by DNS:** DNS blocking reconfigures a DNS server so that it refuses to process particular domain names.[7]
- **URL site blocking:** A URL is used to identify a particular file, directory or server. ISPs can use a proxy server to disrupt the flow of data to a particular URL(s).[8]
- **Blocking by Deep Packet Inspection (DPI):** Packet inspection involves the examination of data packets while they are in transit. Data packets which match certain characteristics (eg IP address) are subjected to a reset command, thereby disrupting their flow.

The four technical measures are illustrated in Ofcom's diagram below.



Source: Ofcom.[9]

Site-blocking does not remove, delete or alter infringing content. It targets the end-user rather than the originator of the content. This may be somewhat counterintuitive but it is key to the rationale behind site-blocking.

THE NEED FOR SITE-BLOCKING

Currently, the Copyright Act provides limited scope for rights holders to obtain a site blocking injunction against ISPs. Under section 116AG(3)(a), a court may require an ISP to *'take reasonable steps to disable access to an online location outside Australia'*. The High Court has, however, ruled that this provision is not enlivened where the ISP has not authorised the infringements.[10] So far, no injunction has been granted pursuant to s 116AG(3)(a).[11]

The current legal framework does not, however, provide a no-fault jurisdiction for rights holders to seek site-blocking injunctions. Instead, rights holders are required to bring an action and establish liability of operators of infringing websites. This is impractical for two reasons.

First, it can be difficult to identify the individuals responsible for a particular website. Unfortunately, the registration system for Domain names and IP addresses is not reliable. There is no verification process to confirm identity when an individual registers a domain name or IP address and in some circumstances, individuals can opt-out of providing identification details.[12]

Secondly, website operators and data servers are generally located overseas; service of process and enforcement of judgement can therefore be complex and costly for plaintiffs.

Litigation in the UK against the Newzbin2 website illustrates both of these problems.

Newzbin2 was a website facilitating online copyright infringement via usenet technology. Newzbin2 was based substantially overseas and the operators of the site identified themselves using pseudonyms – *'Mr White'*, *'Mr Black"* and *'Mr Pink'* – and publicly boasted of their success in avoiding enforcement action.[13] Proceedings against Newzbin2 were therefore impractical because the operators could not be identified and their assets were held overseas.

However, the copyright-owners were able to obtain an injunction against an ISP – BT Telecommunications – relying on section 97A of the *Copyright, Designs and Patents Act 1988* (UK).

>

4 Ofcom, '"Site Blocking" to reduce online copyright infringement: A review of sections 17 and 18 of the Digital Economy Act' (2010) 18.
5 Ibid, 19.
6 Above n 4, 28.
7 Ibid, 32.
8 Ibid, 36.
9 Above n 4, 27.
10 Above n 1, [79].
11 Australian Film Bodies, 'Response to Online Copyright Infringement: Discussion Paper' (2014) at 23.
12 Above n 4, 20.
13 *Twentieth Century Fox Film Corporation v Newzbin Limited* [2010] EWHC 608 (Ch), [58].

Why Australia Needs Site-Blocking [CONT'D]

> To date section 97A's no-fault jurisdiction for site-blocking has been used to obtain injunctions in relation to more than 90 websites.[14]

most empirical studies into file-sharing websites have found that less than 5% of their content is legitimate

Given the real difficulties in taking enforcement action against overseas defendants and the limitations of the current legal framework, the rationale for site-blocking is apparent. However, for any site-blocking regime to be successful, it must be effective, proportionate and fair.

ARGUMENTS AGAINST SITE-BLOCKING

The main arguments against the Government's proposal consist of two key points:

- **proportionality:** that site-blocking may result in unintended loss of access to legitimate websites; and
- **effectiveness:** that it is easy to circumvent site-blocking measures.

While these arguments do not justify an outright rejection of the Government's proposal, they do require that certain amendments and clarifications be made.

Proportionality: Over-blocking

A common argument against site-blocking is that it may result in unintended censorship of innocent websites.[15]

"Over-blocking" can occur for two reasons: first, because of the application of an unsuitable site-blocking technique and; secondly, because of the difficulty of ascertaining whether the "*dominant*" purpose of a website is to facilitate copyright infringement.

A frequently cited example of the first reason is s 313(3) of the *Telecommunications Act 1997* (Cth). This section has been used to block websites connected to criminal activity. On one occasion, *ASIC requested that an ISP block access to an IP address, which resulted in the unintended loss of access to thousands of legitimate websites*. Unfortunately, ASIC's personnel were not aware that a single IP address can host multiple websites.[16]

This example should not be seen to suggest that all forms of site-blocking lack precision. As described earlier, there are four main technical measures of site-blocking available and each has a different degree of precision.[17] In the case of ASIC above DNS-blocking may have been more appropriate because this technique targets a particular web domain (eg www.example.com) and would generally not affect unrelated websites.

Initially, the Government's proposal was unclear as to whether the court would need to turn its mind to the most suitable method of site-blocking.[18] However, the Bill now expressly requires the court to consider (amongst other factors) whether the order would be proportionate and the likely impacts. These factors may lead the court to consider the risk of over-blocking but they do not guarantee that this risk will be considered in every case. Accordingly, the Bill should expressly require the court to consider the risk of over-blocking and to select the most appropriate measure of site-blocking.

The second example of overblocking is the evidentiary difficulty of determining whether a website has the '*dominant*' purpose of infringing copyright. According to Levine most empirical studies into file-sharing websites have found that less than 5% of their content is legitimate.[19] This statistic might suggest that most websites which infringe are '*obvious*' cases. However, in the course of any litigation it may be difficult to analyse all of the content on a website, as many file-sharing and file locker websites contain a vast quantity of material. More to the point, there may be real difficulty in proving that the material is unlicensed.

The plaintiffs would of course, be able to lead evidence that media belonging to *them* has not been licensed to the relevant website. However, they would not be in a position to speak on behalf of other rights holders. The concern is made worse by the fact that the Government's proposal contains no mechanism which ensures that an application for a site-blocking injunction is subject to the usual rigours of the adversarial process. Although the Bill requires applicants to notify the site-operator of the application for site-blocking (or at the very least, take reasonable steps to notify) there remains a real risk that many applications may go unopposed as the site operators would be overseas.

In order to address this risk, it is suggested that the Bill should be amended to allow submissions from parties seeking to represent the public interest and from users whose access to the website would be affected. This should make the process more balanced.

14 BBC, 'Blocked piracy site list more than doubles after ruling', <http://www.bbc.com/news/technology-30234790>.

15 iiNet, 'Submission to the Australian Government Discussion Paper: Online Copyright Infringement', (2014) 20.

16 AIMA Digital Policy Group, 'Submission to the Australian Government Discussion Paper: Online Copyright Infringement', (2014) 8.

17 Above n 4.

18 Australian Government, 'Online Copyright Infringement: Discussion Paper' (July 2014) 6.

19 Robert Levine, 'Free Ride: How Digital Parasites are Destroying the Culture Business, and how the Culture Business can Fight Back' (2011) 55.

Effectiveness: Circumvention of Site-blocking

Aside from over-blocking, the other most frequently raised criticism of site-blocking is that it is ineffective. The Pirate Party claims that *'determined users with basic computer literacy will be able to circumvent any blocking mechanism*.'[20]

There are a number of ways that end users can circumvent site-blocking technology, each with a different level of effectiveness. For example, Virtual Private Networks (**VPN**s) cloak the end-user's geographic location by providing an alternative network route for data and enable users to circumvent all of the four major site-blocking methods, even when the methods are used in combination.[21]

Empirical data on the effectiveness of circumvention techniques is conflicting.

Critics of site-blocking point to evidence that despite seizure of The Pirate Bay's servers in Sweden, there was only a small decline in the total number of IP addresses engaged in piracy, which returned to its average level a few days after the raid.[22] This contrasts with the comments of Arnold J in *EMI Records v BskyB* [2013] EWHC (Ch), who referred to evidence that site-blocking measures against The Pirate Bay had caused its site-ranking (a measure of the site's popularity) in the UK to drop from 43rd to 293rd in less than a year.[23]

Two factors make analysing the empirical data difficult: the readiness to circumvent existing laws or technologies and the availability of lawful alternatives, both of which vary from country to country. In some countries, lawful alternatives may be scarce and circumvention strategies well known, making it harder for site-blocking to have great impact. Other countries may lie at the other end of spectrum.

The *inverse* relationship between the convenience of downloading pirated copies and obtaining a lawful copy demonstrates an important point. Site-blocking will make it more difficult to access infringing sites but its effectiveness will depend on other factors, including the rightholders' willingness to ensure their content is conveniently available to consumers. Lawmakers should ensure that consideration is given to other measures directed at educating and deterring consumers such as a graduated response scheme.

What is clear, however, is that site-blocking does cause inconvenience to end users, whether by having to download encryption software or by having to pay a monthly subscription fee for a VPN service. While site-blocking will not keep out the most determined users, it will almost certainly have an impact on others.

CONCLUSION

The international and anonymous nature of copyright infringement means that there are significant difficulties in taking direct enforcement action against website operators. Site-blocking targets end user access within Australia and is therefore a practical alternative option.

At the same time, the Government's proposal should permit standing for those whose interests are affected (ie end users) or who oppose the injunction on public interest grounds. Currently, the Bill confines standing to the rightholder, the ISP and the site-operator. These modifications will ensure that opposing views are heard. The court should also be required to turn its mind to the method of implementation so that the most effective and least disruptive option is pursued.

Site-blocking is not a panacea but it *will* make a significant difference.

SADAAT CHEEMA is a junior lawyer in the Workplace Relations, Employment and Safety team at Clayton Utz. This paper won the CAMLA Young Lawyers Essay Competition in 2015. The opinions expressed in this paper are the views of the author only and do not represent any organisation.

---

20 Pirate Party Australia, 'Submission to the Attorney-General's Department on the Online Copyright Infringement Discussion Paper' (2014) 3.

21 Above n 4, 41.

22 Variety, 'Pirate Bay Shutdown Has Had Virtually No Effect on Digital Piracy Levels', 13 December 2014 <http://variety.com/2014/digital/news/pirate-bay-shutdown-has-had-virtually-no-effect-on-digital-piracy-levels-1201378756/>.

23 *EMI Records v BskyB* [2013] EWHC (Ch) [106].

CONTRIBUTIONS & COMMENTS

Contibutions and Comments are sought from the members and non-members of CAMLA, including features, articles, and case notes. Suggestions and comments on the content and format of the Communications Law Bulletin are also welcomed.

Contributions in electronic format and comments should be forwarded to the editors of the Communications Law Bulletin at editor@camla.org.au or to

Valeska Bloch or Victoria Wark

C/- Allens
Deutsche Bank Place
Corner Hunter & Philip Streets
SYDNEY NSW 2000

Tel: +612 9230 4000
Fax: +612 9230 5333

CAMLA contact details:

Email: camla@tpg.com.au
Phone: 02 42 948 059
Mail: PO Box 237,
KINGSFORD NSW 2032

About CAMLA

The Communications and Media Law Association Incorporated (CAMLA) brings together a wide range of people interested in law and policy relating to communications and the media. CAMLA includes lawyers, journalists, broadcasters, members of the telecommunications industry, politicians, publishers, academics and public servants. Issues of interest to CAMLA members include:

- defamation
- broadcasting
- copyright
- advertising
- information technology
- freedom of information
- contempt
- privacy
- censorship
- film law
- telecommunications
- the Internet & online services

In order to debate and discuss these issues CAMLA organises a range of seminars and lunches featuring speakers prominent in communications and media law policy.

Speakers have included Ministers, Attorneys-General, members and staff of communications regulatory authorities, senior public servants, executives in the communications industry, lawyers specialising in media and communications law, and overseas experts.

CAMLA provides a useful way to establish informal contacts with other people working in the business of communications and media. It is strongly independent, and includes people with diverse political and professional connections. To join CAMLA, or to subscribe to the Communications Law Bulletin, complete the form below and forward it to CAMLA.

Disclaimer

The Communications Law Bulletin is the journal of the Communications and Media Law Association which is an independent organisation which acts as a forum for debate and discussion and welcomes the widest range of views. The views expressed in the Communications Law Bulletin and at CAMLA functions are personal views of the respective authors or speakers. They are not intended to be relied upon as, or to take the place of, legal advice.

For further information:

Visit the CAMLA website at www.camla.org.au for information about CAMLA, CAMLA seminars and events, competitions and the Communications Law Bulletin.

To: The Secretary, camla@tpg.com.au or CAMLA, Box 237, KINGSFORD NSW 2032
Phone: 02 42 948 059

Name:

Address:

Telephone: **Fax:**

Email:

Principal areas of interest:

I hereby apply for the category of membership ticked below, which includes a Communications Law Bulletin subscription, and enclose a cheque in favour of CAMLA for the annual fee indicated:

☐ Ordinary membership $130.00 (includes GST)

☐ Corporate membership $525.00 (includes GST)
(include a list of names of individuals - maximum 5)

☐ Student membership $45.00 (includes GST)
(include undergraduate full time student card copy)

☐ Subscription without membership $150.00
(includes GST) (Library subscribers may obtain extra copies for $10.00 each + GST and handling)