

13th August 2014

Online Copyright Infringement Consultation
Commercial and Administrative Law Branch
Attorney-General's Department

3–5 National Circuit
BARTON ACT 2600

Submission to the discussion paper on Online Copyright Infringement

Dear Attorney-General's Department,

This submission was written in response to the Online Copyright Infringement Discussion Paper (July 2014)¹ and seeks to answer the questions outlined in the discussion paper as well as raise additional concerns in regards to the proposals. The consultation paper seeks to address the ongoing issue of online copyright infringement by individuals.

As a 17 year old technologically literate individual, I'm increasingly concerned at approach taken by the Government in trying to reduce online copyright infringement. While it is important to acknowledge and resolve the issue of online copyright infringement, it should be noted that copyright infringement will never be mitigated. It is a well-accepted fact that consumers as a whole are far more innovative and adaptive to change than the content producing industry as a whole. While one method of prevention can be implemented by way of legislation and implementation of "reasonable steps", dozens more innovative downloading copyrighted materials will appear.

I believe that legislative changes will have little impact on the way end users obtain their content, but rather, it is the innovation of content producers which will evolve and change the way we consume content in the 21st century. Successful models such as *iTunes* for the music industry have significantly transformed the way regular consumers purchase music. The key to its success is the availability of content, with the vast majority of mainstream tracks and albums available to consumers on one easy-to-use platform.

The cost of implementing a system that is extremely easy to bypass will make this investment of funds an extremely uneconomical investment. It is my belief that content creators and distributors should invest more money on making their data available to more Australians in a legal and simple manner. Until that happens, online copyright infringement will continue to play a major part of Australians' online activities regardless of any "reasonable steps" taken.

Kind regards,
Kenneth Tsang

me@jxeeno.com
www.jxeeno.com

¹ Online copyright infringement—public consultation:
<http://www.ag.gov.au/Consultations/Pages/Onlinecopyrightinfringementpublicconsultation.aspx>

Contents

Proposal 1: Extended authorisation liability	3
Question 1	3
Q1.1 Peer to Peer (P2P) Networks.....	3
Q1.2 Virtual Private Network (VPN)	6
Q1.3 Downloading from a specific server or website.....	7
Question 2.....	10
Question 3.....	11
Question 4.....	11
Question 5.....	12
Proposal 2: Extended injunctive relief to block infringing overseas sites	13
Question 6.....	13
Proposal 3: Extended safe harbour scheme	14
Question 7.....	14
Other questions.....	15
Question 8.....	15
Question 9.....	16
Q9.1 Streamlining of content	16
Q9.2 Content charge equality	16
Question 10.....	17
Question 11.....	17
Conclusion.....	18

Proposal 1: Extended authorisation liability

The discussion paper suggests that sections 36 and 101 of the Copyright Act should be amended to clarify the liability of Internet Service Providers to “prevent or avoid copyright infringement”.

Question 1

What could constitute ‘reasonable steps’ for ISPs to prevent or avoid copyright infringement?

The following section has been separated into key infringement methods and analyses potential mitigation methods and their suitability as “reasonable steps”.

Q1.1 Peer to Peer (P2P) Networks

Peer-to-peer (P2P) networks rely on the use of multiple peers or end users which shares information to one another rather than relying on a central server. This can be used in a file sharing protocol such as *BitTorrent* where a file is divided into smaller parts and each individual peer shares these small parts with other peers on the network until the user has all the necessary parts to complete the file.

Q1.1.1 DCMA Notices

In the context of *peer-to-peer* (P2P) file sharing protocols such as *BitTorrent*, certain content producers currently delegate peer monitors on popular file sharing protocols to determine what users are involved in the downloading of copyrighted material.

The IP address (internet protocol address) of these users can be determined by examining the list of peers (peer tracking) and using reverse lookup of the IP address, the entity to which the IP address is allocated to (this is generally the service provider) can be obtained.

In some cases, these content producers (or their delegates) will send a copyright infringement notice of some nature (e.g. a “DCMA notice”) to the responsible internet service provider in order to rectify the issue. However, due to the nature of *dynamic IP addresses* and its prevalence in Australia, manually processing and determining the end user from the IP address may be a costly exercise. This is particularly the case with reseller service providers who do not necessarily have access to the IP address allocated to end users at any given time.

In the case where a DCMA notice is received by an Internet Service Provider, a reasonable step to be taken would be to contact the end user to notify them “after the fact” of the suspected copyright infringement. This may help reduce and prevent future occurrences of copyright infringements. However, it should be noted that service providers do not currently possess any records to verify the end user’s infringement and would be relying entirely on the accuracy of information located within the DCMA notice as produced by delegates of content providers.

For this process to be enhanced, it may be feasible that a standardised copyright infringement registrar and enforcement protocol could be established in order to streamline and validate the claims of copyright infringement. However, details for such process would be beyond the scope of this submission in response to the discussion paper as it specifically deals with the use of peer-to-peer protocols and IP address records (peer tracking) on an international scale. It would be unreasonable to expect that Australian ISPs keep an ongoing peer list record for the billions of

“torrents” on the public and private domain. Not only is it extremely costly and impractical, but it would also be a waste in investment given the likelihood for alternate P2P networks to be established which would bypass the capacity of these ISP based peer-trackers.

Q1.1.2 Port Blocking or Shaping

The blocking or shaping (that is, artificially reducing the attainable bandwidth) of common P2P “ports” or by using deep packet inspection techniques on internet services is not suitable due to the increasing prevalence of P2P protocols for legitimate purposes. This may include downloading legitimate files such as a Linux operating system image, or using remote backup software such as *BitTorrent Sync* to share files across devices and computers. Since service providers are unable to distinguish between legitimate and illegitimate uses, port blocking and/or deep packet inspection is not a reasonable step to preventing or avoiding copyright infringement.

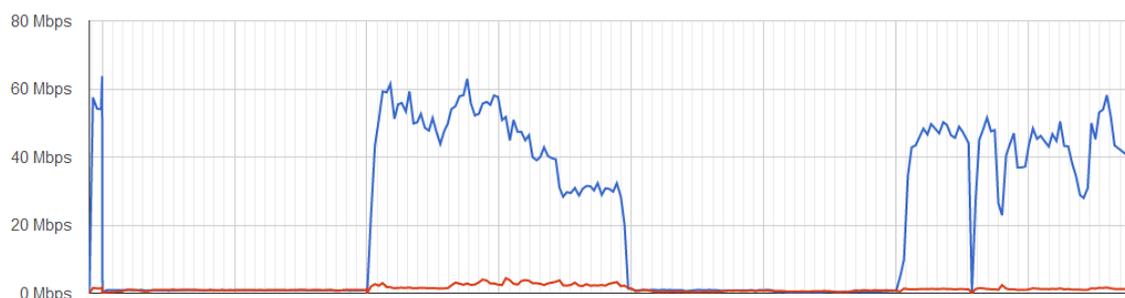
Q1.1.3 Website Blocking

Blocking websites that provide protocol information to P2P protocols such as *The Pirate Bay* has been trialled in other countries such as the UK or Holland. The result of those trials found that site blocking was ineffective in preventing copyright infringement² as new sites or site mirrors can easily be produced. Likewise, third party proxy servers³ may also provide an alternate access route for end users in accessing this restricted data. Hence, website blocking is not a reasonable step to preventing or avoiding copyright infringement.

Q1.1.4 Active monitoring of usage patterns

Downloading from peer-to-peer often carry distinct usage patterns that may be used to determine the use of peer-to-peer networks.

The following chart depicts the usage of a user who utilises peer-to-peer networks. Distinctly, upload and download rates both increase as the end user both “seeds” (uploads to other peers) and “leech” (downloads from other peers) from the network.



However, by analysing the usage patterns of end users as has been demonstrated above, it is insufficient to determine the legitimacy of these uses. The amount of computing power necessary for analysing these patterns would also be unfair on a service provider given that it does not necessarily indicate copyright infringement.

Hence, while active monitoring of usage patterns is suitable for determining the use of peer-to-peer networks, it alone cannot necessarily be used as a reasonable step to prevent copyright abuse.

² <http://www.wired.co.uk/news/archive/2014-01/28/the-pirate-bay-blockade-lifted-in-holland>

³ <http://www.cnet.com/au/news/u-k-s-largest-isp-blocks-the-pirate-bay-but-to-no-avail/>

Q1.1.5 Layer 3 reseller providers

An extra barrier is present for layer 3 (reseller) providers who rely on a managed service by a wholesale service provider such as Telstra Wholesale, Optus Wholesale or AAPT. Depending on the information provided by the wholesale provider, it may not be possible to determine the nature of the data being transmitted and received by the end user.

In the case where the reseller does not advertise their own IP blocks, DCMA notices would not be received by Layer 3 reseller providers. In the case where the reseller advertises their own IP blocks, it may not be possible for them to determine the end user from an IP address provided by a DCMA notice.

Furthermore, the active contracts in place between a wholesale service provider and the reseller service provider (such as a 24 month contract) may prevent the ability for the reseller to terminate the end user's service on the basis of copyright infringement. Under these existing contracts, the liability may fall to the reseller provider to pay for early termination fees.

Q1.1.6 Conclusion

Without substantive analytical processing power of data usage and patterns, Internet Service Providers are unable to determine the use of peer-to-peer networks by their end users. In doing so, the service providers still do not necessarily have the power or ability to determine the copyrighted nature of the data being downloaded or uploaded by end users.

It is substantively possible to conclude that no "reasonable steps" taken by internet service providers can prevent or avoid copyright infringement on the front of peer-to-peer networks. However, it is possible to alert and warn end users after the fact when third party monitors send out copyright infringement notices (such as "DCMA Notices").

Q1.2 Virtual Private Network (VPN)

A Virtual Private Network is a system used traditionally by enterprise or business to extend their private enterprise networks in order to transmit and receive data securely between the private network and a device (or network) beyond that of the secure network. In other words, a VPN generally provides a closed and encrypted end-to-end protocol for connecting from one network to another.

Q1.2.1 Achieving the impossible: decrypting

Once an end user enters a virtual private network and transmits or receives data within this network, a service provider would need to decrypt the tunnelled packets in order to determine the nature of the data transferred. Not only it practically impossible for the service provider to decrypt this data, but it would defeat the purpose of a VPN which is to provide a secure tunnel.

VPNs are commonly used in business, enterprise, military or Government purposes which require high-grade encryption and security. Decrypting (if possible) this data may breach the confidentiality of these transmissions. This should not be the responsibility of service providers and is not a reasonable step to be taken by service providers as they may then be liable for any data leaks as a result of their active monitoring schemes.

Q1.3 Downloading from a specific server or website

Another common source for downloading potentially copyrighted material is from websites over the HTTP or HTTPS protocol. This may be downloading from a specific server containing the copyrighted material, or through the utilisation of file-sharing websites such as *4shared.com*, *Dropbox* or *Mega*.

Q1.3.1 Virtual Hosts Problem

The decline of IPv4 address availability makes it increasingly difficult to block specific websites. Many websites utilise a “virtual host” functionality which utilises a single IP address to deliver multiple websites. This makes it impossible for ISPs to block a specific website using an IP route nulling method without unintentionally blocking other websites (as has happened in the past with S313s⁴), and would require a “transparent proxy” (which increases latency, attainable bandwidth and processing costs) to filter the hostname requested. See Figure 1 below as an illustration of the potential issues of implementing a website filter.

Q1.3.2 Blocking of websites hosting infringing content

Copyright infringing content is published on a variety of platforms including popular file sharing websites (e.g. Dropbox, Google Drive, Box, Mega), video sharing website (e.g. YouTube, Vimeo, DailyMotion) or self-hosted websites. It should be responsibility of these service or platform providers to identify users who upload copyright infringing content rather than the responsibility of Internet Service Providers. Blocking specific files or videos on a popular file sharing website given the large percentage of legitimate uses of these services is an unreasonable expectation for Internet Service Providers.

In cases where copyright infringing material is located, it should be the responsibility of the content host to identify and remove these files from their servers. This is often done through an abuse (or DCMA abuse) complaint process found on host websites.

Q1.3.3 Blocking of websites referring to infringing content

Websites such as *The Pirate Bay* or *mp3skull* contains links or protocol information which links users to a source for retrieving and retransmitting potentially copyright infringing material. Since the website does not contain any actual copyright infringing material, blocking access to these sites while technically possible would be an unreasonable step.

Q1.3.4 Blocking access to websites that facilitate downloading of infringing content

Websites such as *KeepVid.com* may be seen as tools that facilitate the downloading of copyrighted material. Content published on YouTube, unless otherwise stated, is subject to standard copyright law. The legal complexities of “download” (as facilitated by tools such as KeepVid) versus “view” (the legal method of viewing a video using the YouTube website) is in play here.

On a technical level, viewing (or streaming) requires the downloading of the copyrighted material. But for the purposes of KeepVid, it enables the consumer to archive the video for future consumption. However, it would be unreasonable to expect internet service providers to block access to these “tools” as the tools may be used for legitimate purposes (including archiving for the content producer themselves). The legal and technical grey area in the case of downloading vs viewing vs streaming should also be emphasised here.

⁴ <http://www.abc.net.au/news/2013-05-17/concern-over-asic-internet-blocking-bungle/4697236>

Q1.3.5 Conclusion

Blocking specific websites which host and store the copyright infringing content based on a centralised copyright infringing database is, while technically feasible, an extreme measure. There are also certain risks in implementing such filters, especially given technical limitations of transparent proxies. It should also be noted that the effectiveness of “blocking” a website is quite limited given the ease at which a mirror of the old website or an establishment of a new website is for content infringers. Hence, blocking of websites is a reasonable step for preventing copyright infringement for a short term one-on-one basis.

If a website blocking process is implemented, strict guidelines and oversight will need to be implemented in ensure that the mechanism isn't abused (i.e. to ensure it not impede individuals freedom of using the Internet, like the *Great Firewall of China* does).

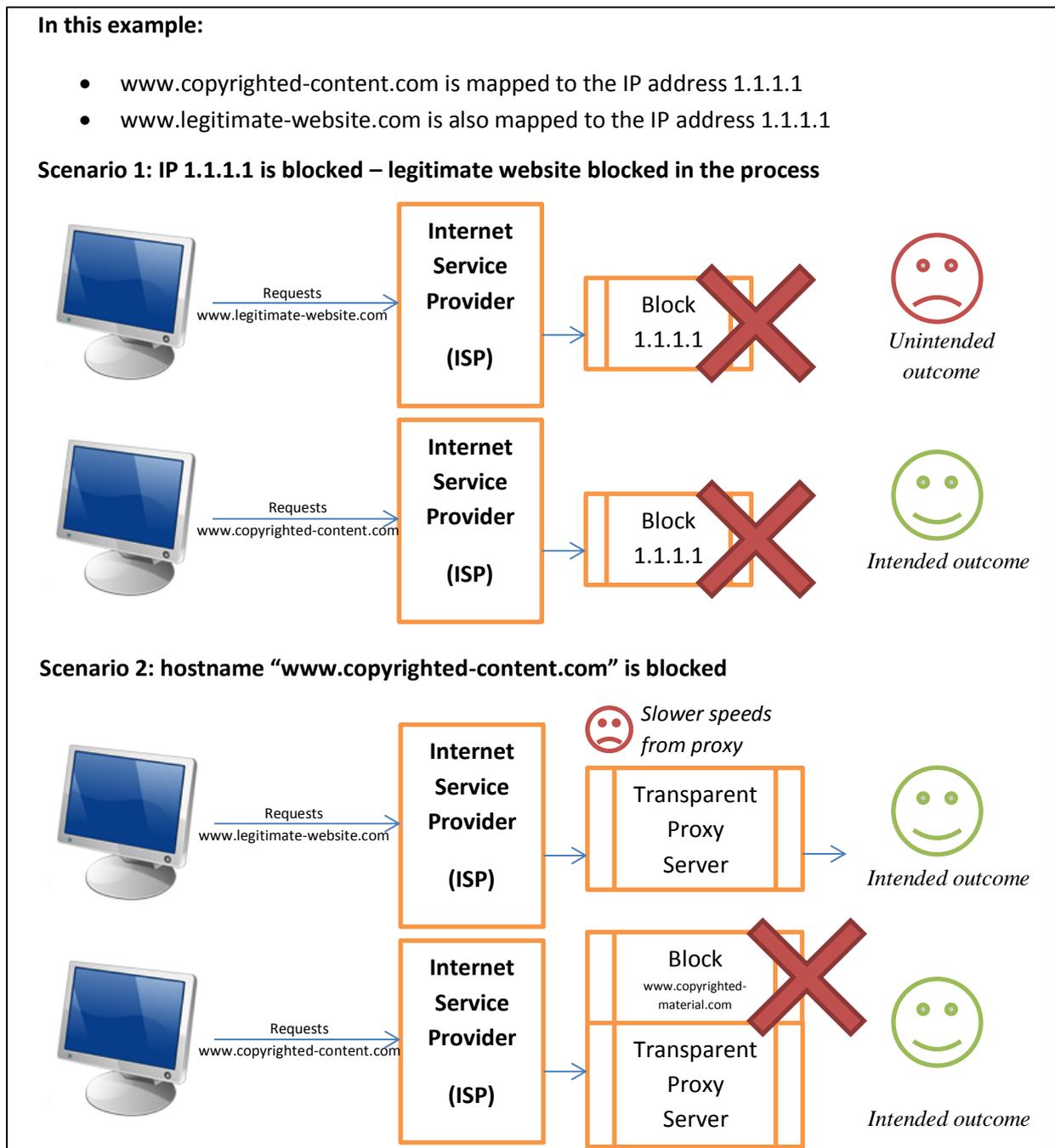


Figure 1: illustrates the virtual host issue in blocking websites

Question 2

How should the costs of any 'reasonable steps' be shared between industry participants?

The cost of internet services in Australia is high when compared with the rest of the developed world. Due to the geographical location of Australia, a limited number of submarine cables carry the vast majority of traffic between Australia and the rest of "the Internet".

With that in mind, I believe that the cost of taking "reasonable steps" should not be directed at consumers, and by inference, the internet service providers. Given the already higher-than-average Internet costs in Australia, it is unreasonable to ask Australians to pay more for their Internet yet still get no additional content.

Furthermore, the costs of mandatory filtering or mandatory analysis of customer usage would bear substantive burden to the functionality and operability of these small businesses especially small internet service providers or network providers.

Overall, however, I believe that money would be better directed at investigating and implementing better content availability and licencing. Availability of consumable content, for example TV shows and movies, continues to be the major barrier for consumers in acquiring legitimate access to copyrighted content. Unlike the music industry where the majority of tracks and music is available on platforms such as iTunes or Spotify, the film and video content industry remains adamant in maintaining monopoly and exclusive content deals with specific content providers. This is seen in examples such as the exclusive rights of Foxtel to distribute *Game of Thrones* in Australia.

Likewise, TV series *Bones* produced by Fox is broadcasted over Free-to-Air TV through the Seven Network. However, the latest season (Season 9) is not currently available to Australians in any of the popular content service providers. This lack of legal content availability Australians is the main driver behind consumers downloading copyright-protected content.

Creative content industry should be responsible for subsidising any costs associated with implementing any "reasonable steps" that may eventuate. Until the content creation industry is able to innovate and agree upon suitable licencing arrangements that benefit themselves and the wider community, the anti-competitive nature and restricted availability of content distribution in Australia remains to be the ultimate cause of online copyright infringement.

Question 3

Should the legislation provide further guidance on what would constitute 'reasonable steps'?

No. Service providers should be given the liberty to decide what "reasonable steps" should be taken.

Given the issue of cost is particularly prevalent for small service and network providers, by enforcing the need for mandatory filtering or mandatory analysis of customer usage would bear substantive burden to the functionality and operability of these businesses.

Question 4

Should different ISPs be able to adopt different 'reasonable steps' and, if so, what would be required within a legislative framework to accommodate this?

Yes. Service providers should be given the liberty to decide what "reasonable steps" should be taken. Please see answer to Question 2 and 3 above.

Question 5

What rights should consumers have in response to any scheme or 'reasonable steps' taken by ISPs or rights holders? Does the legislative framework need to provide for these rights?

As a consumer, I believe that if ISPs or rights holders were to implement a scheme which "prevented" individuals from committing copyright infringements, consumers should be given clear guidance as to what alternative methods are possible in obtaining the same content legally. Given the known barriers of content unavailability and exclusive rights of some monopoly content distributors as outlined in response to Question 2, consideration should be taken in regards to if legal alternatives are available to the consumer.

Frameworks would be necessary to ensure that if consumers are suspected of breaching copyright laws that suitable notice is given. It is important to ensure that consumers continue to have the right to access data, even if it may be copyrighted material, given that the transmission and reception of such data is within the realms of copyright law.

For example, in the case where a consumer is archiving a DVD for personal use onto a protected cloud storage provider, this is not copyright infringement but it may be mistakenly identified as being so in the "reasonable steps" taken.

In the case where a consumer is suspected of breaching copyright laws, it is also important to assess the role of the registered consumer in relation to the access of the data. In a sense, some consumers may be seen as a private "carrier" in their own right.

For example, in the case where an owner of a hostel provides free shared Internet connectivity to its residents, would the owner become responsible for the downloading of copyrighted material?

Proposal 2: Extended injunctive relief to block infringing overseas sites

Question 6

What matters should the Court consider when determining whether to grant an injunction to block access to a particular website?

I believe that the court should consider the following matters:

- Does the website hold a mix of both legal and copyright infringing content?
 - If so, in blocking access to the copyright infringing content, is this blocking access to the legal content as well?
- Is the content of the website infringing in copyright, or does it only facilitate the infringement of copyright?
 - Does this website, if it does facilitate of infringement, assist consumers in accessing data in a legitimate and non-infringing manner such as that identified in Q1.3.4
- Does the website have suitable measures to report abuse or copyright infringement? Does the website work proactively to remove this content?
- Has the content producer attempted to contact the owner, host or network service provider of the infringing website to notify them of the copyright breach?
- Is the website been frequently visited, especially by Australians?
 - Has, as the result of the high visitor traffic to the website, materially damaged revenue to content creators on the basis of lost potential revenue in comparable timeframe.

As emphasised in Q1.3, however, it should be the responsibility of the hosting providers to remove copyright-infringing material from their servers rather than the internet service provider.

Proposal 3: Extended safe harbour scheme

Question 7

Would the proposed definition adequately and appropriately expand the safe harbour scheme?

Yes, by expanding the safe harbour scheme to “service providers” as any person who engages in activities defined in sections 116AC to 116AF, it provides further safe guards to private facilitators and providers who may be at risk of copyright infringement beyond their immediate control.

Other questions

Question 8

How can the impact of any measures to address online copyright infringement best be measured?

A multi-pronged approach to measure copyright infringement is necessary. Some measures of online copyright infringement may be:

Measure	How can it be implemented?	What does it measure?
Peer monitor	Keep a regular monitor and log the number of peers with an Australian IP address who are seeding or leeching from popular content on peer-to-peer networks. Ensure a random and large sample range of popular torrents.	Measures Australians' activity on peer-to-peer networks. Can be compared on a month-by-month or year-by-year basis to variations
Take-up of legal alternatives	Request that content providers such as Foxtel, Quickflix or FetchTV to provide regular updates on customer take-up.	As legal alternatives are taken up by consumers, the less infringement would occur (as consumers would use legal means to acquire the content).

Question 9

Are there alternative measures to reduce online copyright infringement that may be more effective?

Q9.1 Streamlining of content

Content availability, as outlined in response to Question 2, remains the major barrier in Australians taking up legal online content alternatives.

In the case of the music industry, online music stores such as iTunes and Spotify provide almost ubiquitous access for music for the vast majority of tracks that Australians want to listen to.

However, in the case of the film and video content industry, exclusivity and licencing deals means that consumers may need to subscribe to multiple content provider services in order to view TV shows or movies they want. The simple inconvenience of having to find out through each content provider what TV shows or movies they have available leads to a dramatic preference of copyright-infringing options such as peer-to-peer networks.

In the US, companies like Netflix are leading the way in providing a “one-stop-shop” for all video and film content. However, there are still licencing barriers in the United States. The simplicity of having a single search box which allows consumers to download the movies they want to watch is something that the industry should be pushing for. One that can be achieved, many more consumers would be willing to pay that small price to view the content without using copyright-infringing means.

Q9.2 Content charge equality

Traditionally, Australians are prone to price gouging by retailers and content providers. In the past, these additional costs (when compared with acquiring or accessing the same content in other locations such as the US or the UK) were attributed to shipping of material goods and taxation. However, in the case of online content, retailers and content distributors can provide access for anyone worldwide at practically equal cost.

The disparity in local prices and international prices has led to a boom in geo-spoofing utilities such as Virtual Private Networks (VPNs) which allows consumers to mask their location and obtain content at the price of consumers overseas (such as those in the US or the UK).

Without creating a level pricing construct worldwide, local subsidiaries of content providers may find increasingly that customers will use geo-spoofing alternatives to obtain identical content at much lower cost.

Question 10

What regulatory impacts will the proposals have on you or your organisation?

As a consumer, the impact of price rises in phone and internet access is of utmost concern. Given the already high-than-average prices of internet access in Australia, the implementation of “reasonable steps” (if costs are carried onto consumers) will dramatically decrease the viability of Australia as a leading innovation centre – especially in a world that is increasingly going “online”.

Question 11

Do the proposals have unintended implications, or create additional burdens for entities other than rights holders and ISPs?

As stated above in response to Question 10, Australian consumers will have the biggest impact and bear the greater cost burden in the long run. Australian industries that are turning to connect their business to the wider world through the internet will also be impacted by increased prices.

Conclusion

I believe it is beyond the remit of Internet Service Providers to “restrict” access to copyrighted material. It is the responsibility of the providers who host the content to remove this material, not that of a service provider who simply, in layman’s terms, connect consumers to the Internet.

I’ve been unable to find any “reasonable steps” that can be taken by service provider that cannot be easily circumvented or bypassed using simple tools or searches on search engines such as Google.

The technical complexities and subsequently ease to bypass any restrictions implemented by Internet Service Providers make it an unnecessary waste of funds and resources. These funds would be better allocated to making legal content readily and easily available to Australians as iTunes has done for the music industry.

While I applaud the Government in trying to take steps to reduce online copyright infringement, until the content production industry resolves its price gouging and licencing or exclusivity deals, Australians will only continue to increase their online copyright infringements.

Kenneth Tsang
me@jxeeno.com