16 April 2015

Senator the Hon Ian Macdonald
Chair
Senate Legal and Constitutional Affairs Committee
PO Box 6100
Parliament House
Canberra ACT 2600

(Via email: legcon.sen@aph.gov.au)

Dear Senator Macdonald

**Copyright Amendment (Online Infringement) Bill 2015**

The Internet Society of Australia is pleased to provide our submission to your inquiry into the Copyright Amendment (Online Infringement) Bill 2015.

In drawing up this document we have relied on the considerable technical resources available to the Society via its members. This includes lawyers specialising in IT, engineers with expertise in Internet systems design and managers and practitioners who run ISP's and other relevant Internet operating companies.

The consensus of opinion among those with whom we have consulted is that the drafting of the Bill is imprecise in a range of areas that will potentially impact negatively on Internet service providers and their customers.

We do not believe that the legislation will necessarily achieve the Government's stated aims.

The Society would like to offer its expert advice to your committee, in-camera should this be considered appropriate. In that regard, you might be aware that we were invited to assist the Joint Committee on Intelligence and Security when it was considering the Data Retention legislation. We have recently joined an Experts group established by the Attorney General's Department to provide technical advice regarding the implementation of the Data Retention legislation.

Yours sincerely

LAURIE PATTON
Chief Executive Officer


# Submission on Copyright Amendment (Online Infringement) Bill 2015

## 1 Executive Summary

The Internet Society of Australia appreciates the opportunity to make this submission on the Copyright Amendment (Online Infringement) Bill 2015 to the Senate Legal and Constitutional Affairs Legislation Committee.

The Society supports policies that ensure fair reward for creative endeavour regardless of the medium through which the work is made available to the public.

However, we do not believe that this Bill can be justified in pursuit of that objective. We believe that blocking access to international websites will be largely ineffective, being relatively easy to bypass. The costs to the Internet industry and to rights holders to attempt to make blockings more effective will be significant and unjustifiable.

The Bill as drafted is imprecise in many significant areas. This creates real risks that include:

- blocking of access to legitimate sites and content
- causing real economic damage to the owners of legitimate sites blocked in error

Moreover, blocking access to websites could undermine the confidence Internet users have in a reliable, secure and open Internet, a basic precept on which the Internet relies.

The Bill will impose a cost on Carriage Service Providers (CSPs) – and that cost no doubt will be passed on to consumers – at a time when CSPs and their customers are already facing significant expenses to comply with the data retention legislation.

The Bill also fails to adequately describe the consequences and penalties for ISPs should they use methods that are shown to be wholly or partially ineffective in blocking content.

We are further concerned about the possibility of CSPs blocking access to legitimate material that should not be subject to this Bill simply due to the risk of high costs in appearing in court to defend demands to do so.

This latest Bill is little different from the proposed mandatory Internet Service Provider Content Filtering proposal introduced in 2009.

Several independent technical trials of content filtering performed for ACMA at the time found that Internet performance slowed by between 2 percent and 75 percent depending on the variety of content filtering equipment trialled (essentially blocking websites, just as this Bill envisages). The increased performance and speed expectations of Internet connections six years later, especially with the high speeds being made available via the NBN, can only accentuate the detrimental effect that such equipment will have on modern broadband connections.

## 2 Ineffectiveness of Blocking Websites / Locations

We submit that the Bill will not prevent access to a vast array of allegedly infringing material available on the Internet either because it is delivered by means other than "the web", because the URL of the material varies with each access, or because many users bypass the systems ISPs might use to control access.

While the Bill provides for blocking websites which form directories and lists of links to infringing material, it is not necessary for a user to access such a site in order to commence downloading the infringing content itself. The infringing content is rarely stored on the same servers with the same names as the index sites – they are stored elsewhere, and most often are distributed across other users' platforms. Such content can be accessed without any reference to any index that might be blocked under this legislation.

With the ease of changing domain names and IP addresses, any list of websites or locations that refers to these site attributes can never be considered as either complete or current. It is likely to be out of date within hours of being listed in an injunction, leaving the content and index material still available.

Furthermore, while the intent of the Bill appears to be aimed at content available using the World Wide Web protocol ad 'websites', much of the content and index material is available through a wide variety of other protocols and systems. It is not feasible to filter traffic accessed through the array of alternative communications protocols and methods, such as HTTPS, peer-to-peer, instant messaging, including any sites using dynamic database-driven content where the URL varies with each access.

The method used by ISPs to implement an injunction to block an international website is also important. One commonly proposed method to perform such blocking is for ISPs to implement a 'DNS block', where the name of the website is translated to a different numeric Internet address when the user's computer queries the ISP's name translation server.

Unfortunately many users' computers do not use their ISPs name translation servers to perform this translation, which is instead done using international servers outside the jurisdiction of the injunction. For instance, many anti-virus software systems replace the ISP's servers with the antivirus company's servers as a security measure. Such users will be completely unaware and unaffected by the block requested by an injunction, and will continue to be able to access the offending site and content.

In addition, the global Internet technical standards community has been progressively deploying cryptographically secure name translation systems (DNSCRYPT and DNSSEC) over several years specifically to detect and prevent tampering with the name-to-address translation.

These measures increase the security and confidence of Internet commerce and general use. This Bill, without more specific guidance, may simply be asking ISPs to attempt to perform the very activities that Internet cybercriminals attempt, and for which these measures were designed to prevent – a futile situation.

We submit that CSP blocking of alleged infringing material hosted overseas will be largely ineffective, and will be easy to bypass.

It may have the perverse effect of requiring ISPs to mimic cyber-criminals, with the decrease in trust and confidence in Internet use and commerce that this entails.

# 3 Detrimental Impact on ISPs and Internet Users

We submit that this Bill creates a real risk of slowing the operation of the Internet for a wide range of users and is likely to drive up Internet service charges.

A report prepared by the Internet Industry Association, commissioned by the Commonwealth Government[1] stated among its key findings:

> *Australia has a very heterogeneous ISP industry. Depending on the nature of a mandated filtering function, the impact on industry may be significant.*

A media report from 2010[2] cites ISP estimates that systems to implement mandatory web content filtering could cost several million dollars, and would need to be refreshed with a small number of years as traffic levels grew, although other estimates were smaller.

A report prepared by Ovum commissioned in 2003 by the then Communications Minister recommended that the Government should subsidise the scheme and assist small ISPs with the capital and management costs, similar to the recent undertakings regarding the Data Retention Bill.

Any ISP costs to install and operate web content filtering and blocking equipment under this proposed legislation is likely to be passed on to consumers through higher Internet service costs, decreasing the online economy benefits for all Australians.

---

[1] "Feasibility Study – ISP Level Content Filtering", IIA, Feb 2008, available online at http://*sydney.edu.au/engineering/it/~bjornl/Main_Report_-_Final.pdf*

[2] D Pauli, "Net filters could put ISPs $1M out of pocket", Computerworld, 10/03/2010, online at http://www.computerworld.com.au/article/339063/net_filters_could_put_isps_1m_pocket/

This Ovum report (no longer available on the Internet due to the closure of the DBCDE website) also outlined Internet performance degradation, depending on the method of blocking used, of between 2 percent and 7 percent, especially during peak traffic periods.

Internet content blocking systems also cause the Internet reliability to be reduced by forcing all traffic to bypass through the filtering system. Internet services achieve high reliability largely through having no single point of failure – traffic generally has many possible paths that it may take to travel from source to destination and can route around a fault or failure in one path. By mandating that all content traffic must pass through a filtering point to be inspected and blocked if necessary, the resilience of services is decreased, causing increased costs for ISPs, for instance in staffing call centres to cope with the increased loads of complaints during a failure or congestion incident.

# 4 Applications for Injunctions Unlikely to be Opposed

The Bill provides a strong financial incentive for CSPs not to appear in proceedings by rights holders seeking an injunction. CSPs will not be liable for costs unless they take part in the proceedings.[3]

The likelihood is that rights holders will seek an *ex parte* injunction, joining multiple CSPs in the proceedings. Because the Bill provides a strong incentive for CSPs not to take part in the proceedings the matters that a Court must take into account when granting an injunction[4] will often not be challenged by CSPs.

In addition, because the parties to any proceedings can only be the rights holder(s), the CSPs and the person who operates the online location (if they have applied to be joined to the matter), other interested parties or organisations will not be heard unless they are prepared to bear the costs of such participation.

Without evidence to the contrary it will most probably be left to the Court to determine whether:

- the online location does make available either the copyright material or means to access the material
- disabling the access is a proportionate response
- the granting of an injunction will have a detrimental impact on persons or classes or persons

In many cases the Court will not have access to the detailed technical and operational expertise that might be required to properly form a view as to some of these criteria.

---

[3] Copyright Amendment (Online Infringement ) Bill 2015 cl 115A(9).
[4] Ibid cl 115A(5).

## 5 Potential for legitimate content to be incorrectly blocked

The Bill as currently drafted requires an ISP to block access to "an online location" with no further definition as to what an "online location" might be.

What appears as a single web-page might be one of hundreds or thousands of unrelated pages and entire websites served from a single physical or virtual web page server. If the phrase "online location" is interpreted to mean the server on which the content is located, and access to this machine is blocked, then all the other unrelated sites and web content will be blocked as well, causing significant unintended "collateral damage". Such an interpretation could be exploited by criminals and vandals to implement denial-of-service attacks on significant commercial infrastructure being served from public "cloud" platforms, through creating an infringing site designed to trigger a blocking injunction.

This precise situation occurred recently with the inadvertent blocking of thousands of websites by a Government agency using the provisions of Section 313 of the *Telecommunications Act 1997*. This highlights the need for agreed technical processes for the blocking of sites/locations to ensure that only the intended site or location is blocked.

As an injunction will be sought to completely block access to a site, all access might be denied including access to other content on that site that may be acceptable under Australian copyright law.

**Recommendations**

**Clause 115(5) be amended to add an additional matter: *The impact of an injunction on legitimate access under Australian copyright law to other material, whether related or unrelated, located at the same online location.***

## 6 Impact on CSPs Regarding "Reasonable Steps"

The Bill will require CSPs to take "reasonable steps" to disable the online location.[5] Without further guidance, it is unclear as to what CSPs should do to block access to locations or sites. As outlined above, depending on the method used there will be significant variations in effectiveness, cost, and 'collateral damage' blocking of legitimate content It is also unclear what processes undertaken by a CSP will be considered as having been reasonable and by whom. This is particularly important because, as discussed above, CSPs are often unlikely to be parties to the proceedings for an injunction and therefore, not present to discuss what will be considered reasonable in the circumstances.

[5] Ibid cl 115A(2)

**Recommendations**

**That the Government convene a working party that includes CSPs and others with technical expertise to set out what steps CSPs should take to meet the test of "reasonable" under the Bill, while ensuring other sites/locations are not blocked.**

**That the Government provide financial assistance for CSPs in developing and implementing agreed processes for blocking access to sites/locations.**

# 7 Notice for Blocked Sites

For every site/location that is blocked, there should be a redirection notice activated whenever any person attempts to access the site that includes at a minimum the following information:

- notification that the site is blocked by the CSP
- the time and date of blocking being requested
- a statement that the site is blocked pursuant to a court order
- the name of the rights holder(s) that sought the court order
- contact details of the CSP
- the process that the viewer should follow to have the block reviewed or removed

There must also a process whereby CSPs can deal quickly with any cases of inadvertent blocking so that access to the site can be quickly restored.

**Recommendation**

**That when a site/location is blocked, there is a redirection notice with full details provided and that CSPs develop processes to deal quickly with complaints about inadvertent site blocking.**

# 8 Review of Operation

Because, in our view, blocking of sites/locations will be neither practical nor effective, we recommend that the Bill is reviewed at the end of its first year of operation.

**Recommendation**

**That the Government review the effectiveness of this Bill one year after its enactment. The review should include the number of sites/locations blocked, the number of sites/locations that continue to provide access to alleged infringing material, the costs to CSPs of implementing requirements of the Bill, and the practical effectiveness and ease of bypass of the methods used to implement blocking.**

About the Internet Society

The Internet Society of Australia is the Australian chapter of the worldwide Internet Society and is a not-for-profit organisation founded in 1996. Our mission is to promote Internet developments for the benefit of the whole community, including business, educational, professional and private Internet users.

Our directors and members hold significant roles in Internet-related organisations and enable the Society to provide high level policy and technical information to Internet user groups, governments and regulatory authorities.

Globally, the Internet Society coordinates Internet policy development and technical standards. This includes advising the United Nations and international Internet management organisations such as the Internet Corporation for Assigned Names and Numbers (ICANN) and the five Regional Registries. The Internet Society assists the Internet Engineering Task Force. See: www.internet.org.au