Singapore/Hong Kong
7 April 2021

Ministry of Law
Singapore
By Email: MLAW_Consultation@mlaw.gov.sg

RE: Feedback on Draft Copyright Bill in Response to MinLaw's Public Consultation

The Asia Video Industry Association (AVIA) warmly thanks the Ministry of Law for the opportunity to comment on its draft new Copyright Bill. As the Ministry is aware, our Association has been deeply concerned about the prevalence of unauthorized video streaming in Singapore, and we are optimistic that the current draft provides an opportunity to substantially improve Singapore's legal framework for tacking this problem. We also express our appreciation for the Ministry's continued active engagement with industry in this process.

The Asia Video Industry Association is a non-profit trade association of 80+ companies dedicated to promoting the health and prosperity of the television industry and professionally curated streaming video services across Asia Pacific. The members of AVIA have extensive experience in building and creating television and video content and infrastructure to meet the needs of populations across the region. Our membership consists of a combination of local, regional and multi-national companies and a very large percentage have based their Asian operations in Singapore, and form an essential part of Singapore's media ecosystem.

Our principal focus in the proposed new Copyright Law is its effort to provide for civil and criminal remedies against parties dealing in illicit streaming devices (ISDs) and illicit streaming apps for commercial gain – viz sections 141 and 142 of the new draft and related sections such as 148 and 418.) We strongly support this policy direction, and we would like to offer some practical assistance, aimed at ensuring the new Copyright Law functions with minimal friction to achieve the policy goal.

Defining the Conduct to be Rendered Illegal

The Ministry's draft of Sections 141 and 142 proposes to establish the illegality of ISD transactions by having the courts assess an ISD's links to "flagrantly infringing online locations" (FIOLs) and the awareness of such links to the FIOLs by the parties dealing in such ISDs and apps. We understand why the Ministry is proposing this – the concept of an FIOL is already established in Singapore law and has been smoothly implemented by the courts in various site blocking cases.

However, we do not believe that the approach of having courts look for connections between ISD retailers/importers/servicers and FIOLs will in the end be helpful to the smooth functioning of the Copyright Law or effective in practice. Introducing the FIOL construct into the assessment of the infringing nature of an ISD will result in impractically heavy evidentiary thresholds, and will also create significant uncertainty about whether the provision can be applied in the real world.

Our view on this is grounded in the contrasting technical aspects of the operation of illicit streaming websites on one hand, and ISD boxes and apps on the other.

- Illicit streaming websites tend to operate in a straightforward manner. The FIOLs associated with such streaming sites tend to be the domains or IP addresses which are used by end-users to access the pirated content offered at these sites. While the FIOLs can and do easily shift domains, the need to ensure that end-users can know of these new domains in order to continue to access the illicit streaming site means it remains relatively easy to identify the domains and IP addresses used by the pirate operators, and which stream the infringing content. This is the information that is required in order to execute blocking via DNS servers.
- ISDs and apps operate in a technically much more complex environment. There is no single FIOL which is associated with such ISDs and apps. Instead, there are a variety of online locations which are associated with various functionalities, all of which contribute to the operation of and ISD/app. For example, one online location may host an authentication server that verifies the box/app's credentials to access the service. Another might host an EPG server that provides info as to what programming is available. A further one may host an update server that is accessed by the box/app to determine if software updates are necessary, and manage the update. All of these are separate from the numerous content servers in widely separate domains or IP addresses that actually stream the content. A single box/app is likely to access many different online locations and these can actually shift dynamically in response to network conditions.

(The above is a brief summary; we earlier shared a more detailed analysis of the technical aspects with MinLaw and IPOS and will be happy to provide other briefings if necessary.)

As the individuals and syndicates who operate the infrastructure of the ISD/App will often have little or no connection with the retailers who offer for sale or distribution such ISD boxes and apps, such retailers are likely to have no knowledge of precisely which online locations are associated with any ISD/App, nor which FIOLs "facilitate" access to the content. All the retailer will probably know is that the box/app provides a user with access to infringing content, and he/she then markets the ISD or app for that purpose. Requiring that the retailer be proved to have actual knowledge of the FIOL would make prosecution exceedingly burdensome for the prosecution (in criminal proceedings) or the plaintiff (in civil proceedings).

Similarly, requiring notice to the owners/controllers of domains or IP addresses is impractical, given the complex nature of infringing content supply to users of ISD boxes and apps, and also meaningless as such owners/controllers of the domains (who are often based outside of Singapore) will have little or nothing to do with the retailers which would have committed the relevant infringements/offences in Singapore.

We would suggest, therefore that MinLaw remove the references to FIOLs in the proposed new law. It should be possible to find an approach that avoids having to address the source of the infringing programming made available by an ISD. As a possible replacement, there are several alternatives that could be considered.

- MinLaw could take reference from Taiwan's newly-amended Copyright Law, written to proscribe trade in ISDs. The Taiwan approach requires that the retailer be shown to have the intention to

make profits by knowingly selling devices, software or services **that access infringing IP**. (The Taiwan text and an English translation are attached as Annex 1.) (Note: We see all over the world that governments take reference from each other's legislative work in attempting to design approaches to complex new issues posed by technological change. This is also consistent with the global goal of inducing more copyright compliance worldwide, as the digital world is effectively borderless. This is the reason we suggest that MinLaw might consider taking reference from Taiwan's approach.)

- MinLaw could look to use similar language to Section 48 of Singapore's Broadcasting Act, which makes it a crime to "manufacture, assemble, modify, import, export, sell, offer for sale, let for hire or otherwise distribute any decoder *which he knows* is an unauthorised decoder" (emphasis added). The decoder is "unauthorised" if it "enables an encrypted programme to be viewed in decoded form *without the authorisation of the lawful provider* of a broadcasting service who had broadcast the programme." This is notable in its connection of the knowledge requirement to "the (lack of) authorization of the lawful provider," rather than requiring courts and prosecutors to address where the encrypted stream might have been obtained.

In either of these cases, the link is not to a specific infringing online location, but to the function of the device (or app) itself, i.e. being used to access the copyright work. The knowledge element on the part of the offender which has to be proven is also linked to the knowledge of accessing such infringing content (which would notionally be more straightforward to prove), as opposed to the need to prove knowledge of an online location which such offender would neither need, nor be interested to know.

Looking at similar provisions already used within the Copyright Act, while Section 136(4) is not necessarily ideally suited to taking action against ISD sellers, nor particularly future-proof, the language is helpful in terms of its simplicity – it makes it an offence to make or possess an article "**designed or adapted for making infringing copies"** of a copyrighted work.

Whilst we understand that there is a concern that the proposed legislation could theoretically be applied in an overly broad manner to potentially capture non-infringing devices such as a Smart TV or any plain vanilla Android device, we suggest that even if the concept of an FIOL in the current draft was replaced with the concept of "facilitating access to any work without the authorization of the rights owner", the provisions as drafted would still be targeted against persons dealing with illicit devices or Apps as it would still be necessary to show

> the person knows or has reason to believe, that the device or service —
> (i) is promoted, advertised or marketed as being capable of facilitating access to any work without the authorization of the rights owner;
> (ii) is able to facilitate access to any work without the authorization of the rights owner in the ordinary course of operation of the device; or
> (iii) is specifically designed, made or performed (as the case may be) primarily for the purpose of facilitating access to any work without the authorization of the rights owner;

We understand that the legal counsels for some of our key member companies will be providing further information on these possible alternatives in their submissions.

Criminal versus Civil Proceedings

We would ask that MinLaw implement the policy determination to criminalise ISD-related commercial activities by providing a straightforward criminal offense, rather than to require rights holders to rely on section 418 which also requires the additional elements of willfulness of the infringement and commercial advantage to be established. This is in contrast to other specific copyright offences (e.g. Clauses 417, 419, 421, 424, etc), where such additional thresholds do not have to be established.

Enhancing the Injunctive Relief Process for Site Blocking:

A June 2020 survey on online content viewing behavior in Singapore found that 17% of Singapore consumers and nearly a third (32%) of 18 – 24 year olds access streaming piracy websites or torrent sites. The survey, commissioned by the Asia Video Industry Association's Coalition Against Piracy (CAP) and conducted by YouGov, also found that 10% of consumers use an ISD to stream pirated content.

Despite the unhealthy appetite for accessing piracy services, the YouGov survey also found that the overwhelming majority (86%) of those surveyed recognised that online piracy had negative consequences. Other results showed 53% of online consumers were of the view that online piracy increases the risk of malware infections on computers and devices, 52% recognised that crime groups financially benefit from the stolen content, and 42% were concerned that piracy puts the livelihood of those who work in the creative industry at risk.

When asked who should be responsible for preventing online piracy in Singapore, consumers were of the view that the individuals (by choosing not to buy/watch pirated content) were the most responsible with the Singapore government deemed the second most responsible.

Review of the Status of Site Blocking in Singapore:

Overseas-based pirate sites, outside the jurisdiction of Singapore law enforcement, continue to drive this illicit consumption. As such, site blocking remains a key remedy to disrupt and limit online piracy and if applied in a time-effective manner it can migrate consumers back to reliable and safe legal services. By way of example, Indonesia has become market leader in video IP protection in South East Asia[1] by enforcing a time-effective "rolling" site blocking system and boosting the growth of legitimate services. Traffic[2] to piracy sites dropped by an estimated 74% (August 2019 to February 2021) with traffic to legitimate video sites increasing by an estimated 150+% within the same period.

In the last few years Singapore's site blocking remedy has been put to good use and is making a material difference to mute the previously rampant growth of online piracy in Singapore. The site blocking remedy has been shown to change consumers' behavior. The June 2020 YouGov survey also found that

[1] https://www.bloomberg.com/news/articles/2021-03-03/disney-dis-netflix-nflx-battle-piracy-in-southeast-asia
[2] AVIA/CAP study based on traffic data from Alexa. The data is indicative and not absolute.

20% of online Singapore consumers had noticed a piracy website or ISD application that had been blocked. Of these consumers, 62% said that as a result of piracy websites being blocked in Singapore that they would no longer access any piracy sites; 20% said they would now 'only rarely access' a piracy website; and only 18% admitted that it made no difference to their viewing habits and they would find an alternative piracy website.

However, despite this encouraging consumer feedback, piracy remains a critical problem for our industry in Singapore and continues to have a profound impact on the media economy of Singapore with job losses rising, innovation stifled and very significant amounts of money defrauded from rights holders and tax payers.

We have two primary requests for consideration:

1. We humbly request consideration that the injunctions be broadened to ensure that rightsholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.
2. There is an urgent need to increase the time-efficiency of Singapore's site blocking remedy by allowing for a more time-effective site blocking process. This concern applies to all types of content, but particularly live events or sports, where time is of the essence in blocking access. To this end we would propose the following adjustment of the current notice procedures to reduce the current estimated three month "minimum" time-frame it takes to secure blocking orders, whilst still ensuring appropriate notification safeguards remain in place.

    a) **Removing the 14 days procedural requirement of the Form A 'Take Down' request to website owners:** From the Second Reading Speech[3] by Senior Minister of Law Indranee Rajah SC on the Copyright (Amendment) Bill, 7th July 2014, it would appear that one of the key reasons for the need to provide the Form A notice to the owners of websites which rights owners are looking to block, is to ensure that the "*website owners must also be notified of the application so that they too have the opportunity to present their case before the Court*" (see para 74). The other, is to provide for some time to allow the website owner the opportunity to cease the use of the website in question for infringing purposes.

    With regard to the provision of an opportunity to the owners of websites to present their case before the Court, such objective would be sufficiently satisfied when the website owner is notified concurrently with the filing of the site blocking application, given that there is usually a reasonable amount of time between the date of the filing of the case, to the date of the hearing of the case before the Court.

    With regard to the need to provide for time to allow the website owner the opportunity to cease the use of the website in question for infringing purposes, in reality, such infringing websites often make an effort to be anonymous. Very few infringing websites maintain

[3] https://www.mlaw.gov.sg/news/parliamentary-speeches/2r-speech-by-sms-on-copyright-amendment-bill-2014

legitimate points of contact[4] and are often hidden behind third-party intermediaries. Moreover, to our knowledge, of all the site blocking actions that have taken place in Singapore since the implementation of this remedy, there has not been any website owner that has chosen to cease the use of the website for infringing purposes.

In light of the above, the 14 days Form A requirement has not served much purpose, other than to add to the lengthy time frame it takes to apply for a blocking order and thus reducing the efficacy of this remedy. We would thus request that this 14 day Form A requirement be removed.

b) **Removing the procedural requirement of the Form B 'Notice of Intention to Apply for Order to Disable Access to Online Location":** The Second Reading Speech at paras 70 and 71 ("Notice to the network service providers and website owners and right to be heard") states that:

> 70. First, the Act requires rights holders to notify network service providers of their intention to apply for a blocking order.
>
> 71. This allows the network service providers the opportunity to resolve the matter out of Court.

S 193DDA is a no-fault injunction which also requires the court to recognize that a website is a "flagrantly infringing online location" before a blocking order can be considered. As such there is no matter that needs to be, nor can be, resolved by plaintiffs and NSPs "out of court". Thus the Form B would appear to be redundant and merely adds to the additional time-frame required to apply for the court order. We would thus humbly request that the Form B requirement be removed.

c) **Adjusting the evidential requirement to show that an FIOL is available on all NSP networks:** This is an onerous forensic process which adds to the plaintiffs' cost and time to collate such evidence. Previously blocked FIOLs have always been overseas-based pirate sites, and if available on one NSP would generally be available on all NSPs. This is not an evidential standard that is required in Australia (whose injunctive relief legislative framework is similar to Singapore's).

d) **Statutory Dynamic Injunctions**: To legislate where an FIOL has been ordered to be blocked, rightsholders shall be entitled to notify NSPs in writing in instances where such FIOL is subsequently made accessible via a different domain name server, IP address or URL, whereupon the NSPs must apply such blocking orders issued by the court to these new domain name servers/IP addresses/URLs and disable access to them as soon as possible, unless NSPs raise any objections.

[4] In the HC/OS 399/2020 site blocking case, only seven (7) of thirty four (34) FIOL domains provided a web browser URL point of contact. Other than one "automated reply" from a web browser, the plaintiffs did not receive any correspondence from the 7 domain FIOLs contacted.