Comments in Response to the IPO's Request for Views on
The Illicit Streaming Device (ISD) Industry

April 7, 2017

CASBAA is the non-profit association of the international pay-TV industry in the Asia-Pacific region. CASBAA is dedicated to the promotion of multi-channel pay-television via cable, satellite, broadband and wireless video networks. Founded in 1991, CASBAA currently represents about 100 member companies, located in 17 Asian countries and regions. In addition to multinational television networks and programmers, member corporations also comprise pay-TV retail service operators, leading suppliers of cable, satellite, and broadband technology, related business service providers, telecom companies, and new media service providers. Taken together, they have extensive experience in building and creating television infrastructure and quality programming to meet the needs of this region's more than 500 million multichannel TV households.

CASBAA's membership is diverse, including many indigenous Asian companies as well as European and North American-based corporations. Britain's major content providers play leading roles in the Association, including BBC Worldwide, ITV plc, and the Premier League.

We are grateful for the opportunity to give the IPO our views on certain global aspects of development of the Illicit Streaming Device (ISD) industry. Unfortunately, we now have had to amass considerable experience with these devices and the syndicates which sell them and operate the content networks on which they rely. However, as the focus of our activities comprises Asian legal jurisdictions (and not the UK), our knowledge of the legal framework and specific enforcement constraints in the UK is limited. We therefore will confine our answers to certain of the international questions posed by the IPO in its Call for Views. We believe the IPO will find it useful to understand developments in Asian markets, which were the first to be affected by ISD-based infringement.

Answers below are keyed to the question numbers in the Call for Views paper.

Difficulties in evidence gathering

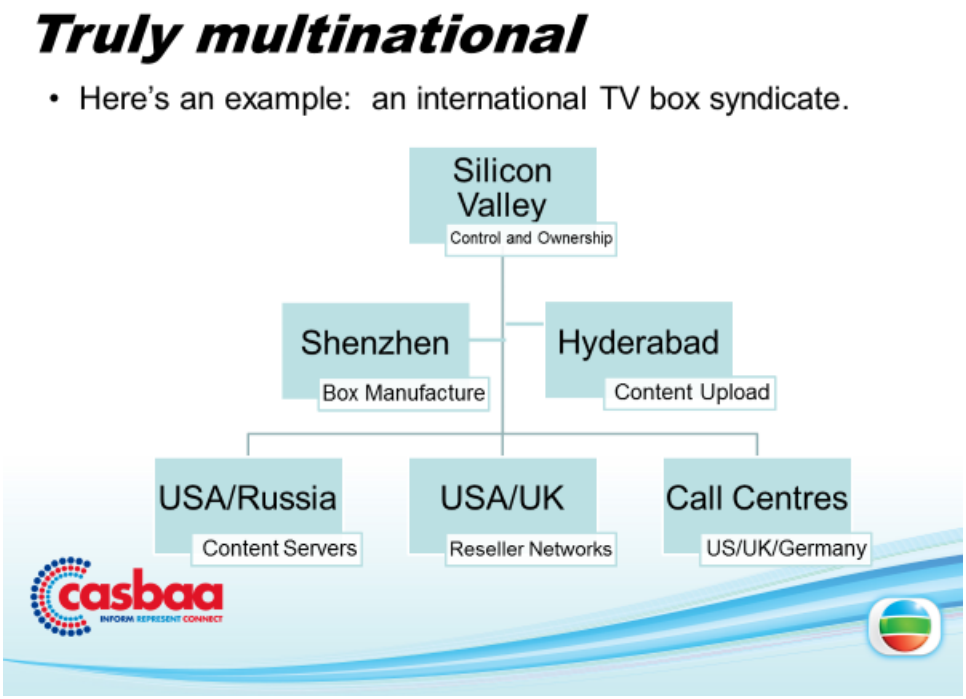
> ***Q6: Are there any issues around evidence gathering for these existing offences? This could arise conceivably from the need for digital forensic capability, or the often dispersed nature of the illicit streaming infrastructure.***

There are considerable difficulties in gathering evidence that might lead to effective enforcement action against ISD networks. The roots of these difficulties lie in the often transnational and compartmentalized elements of the ISD ecosystem. The low cost of broadband video transmission plus the desire of the syndicates to hide in non-cooperative enforcement jurisdictions has meant that the largest and most damaging ISD networks are usually spread across several different countries and the nature of their connections is often intentionally obfuscated.

By way of example:

1. Content X that may be illegally retransmitted in country A is often sent to servers and content delivery networks located in country B, for retransmission to users located in countries C,D,E,F, etc.
2. User access to content X is made possible by way of EPG and authentication servers which may be located in country G.
3. The Android TV boxes which facilitate access to the EPG and authentication servers may have been manufactured in country H.

The following diagram (used in a previous briefing for the IPO) illustrates the highly multinational nature of a typical ISD conspiracy, based on an enforcement action undertaken in India in 2014.



To this should be added nodes for operation of financial payment processing (for subscription-based services) and advertising placement (for ad-based services.)

Investigating and launching enforcement action against such a many-headed hydra is both complex and expensive. Removing one part of the conspiracy can simply result in growth of a new limb to replace it. Therefore additional difficulties in the evidence-gathering process would include:

- Detailed forensic examination of the ISD is required in order to trace the various components of the network and understand at what node the infringing nature of the activities are taking place, in order to decide an effective enforcement strategy that can comply with existing outmoded legal frameworks. Such forensic examinations are rendered more complex because of the obfuscation techniques that syndicates can deploy.
- In order to forensically analyse the ISD, a wireless network point will need to be established on a standalone computer and connected to the ISD, thus making the standalone computer able to monitor all network traffic to and from the device. Only then can one establish an understanding of the data traversing the ISD and determine the important servers that are responsible for providing functionality to that device.
- We have observed that the general flow of communication from an ISD is often thus:
  a) The ISD performs a DNS lookup for the authentication server.
  b) The DNS server responds with the IP address of the authentication server.
  c) The ISD requests authentication, with MAC address, userID, and serial number of the device itself.
  d) Upon authorization, the server provides confirmation details and time before subscription expiry (assuming this is a subscription service, which is not uncommon in Asia.)
  e) The ISD requests EPG data from the EPG server.
  f) The server provides EPG information, which is displayed to the user.
  g) The user makes a request to the EPG or P2P server for channel/VOD stream to commence.
  h) The EPG server communicates with the relevant content server (which is often obfuscated from any remote forensic examination, as the infringing content resides there). The content for one ISD box or app may be stored in multiple locations in various countries.
  i) Transmission of the channel or VOD content commences.

- In many cases, the syndicates are organized around hardware, software, and service suppliers who may also have large legitimate lines of business, and they do not wish to have attention drawn to their illicit activities. Thus, they intentionally obfuscate their roles within the ISD ecosystem.
- CASBAA is of the view that for cultural reasons (lack of respect for IP laws and willingness to countenance sub rosa activities), otherwise-legitimate companies rooted in certain Asian and Eastern European countries are particularly prone to pursue the dual roles of suppliers of legitimate and illicit services[1].

[1] An example already in the public record of a company with such dual roles is the case of Zhuhai Gotech Intelligent Technology Co. Ltd, which was the subject of a verdict in the Southern District of Texas for illicit activities that saw

- Given the structure of this ecosystem, frequently the only physical presence of an ISD syndicate in-country is made up of the many resellers of the ISD boxes. The syndicates make use of wide networks of small entrepreneurs to achieve broad retail penetration of ISDs. The boxes are sold wholesale to resellers who then on-sell in small shops or using online e-commerce or social media platforms. The dispersed nature of retail sales increases the evidentiary burden and also the expense of trying to achieve definitive repression of an ISD syndicate.
- Effective border control by customs services is rendered more difficult because the ISD boxes themselves may be manufactured as "clean" devices, with no illicit applications uploaded to the device until after it has passed customs controls. The illicit applications are then added at a subsequent point in the distribution chain – perhaps by the reseller. (This mode of operation seems to have expanded in recent years, as the syndicates have sought ways to evade both customs rules and Chinese government technology/content control licensing rules which affect set-top boxes.)
    - In our experience in China, this manufacture of "clean" boxes is an expedient designed to evade enforcement by local authorities. (This is a major differentiating factor between this industry and, for example, the Android mobile-phone industry – both sets of devices operate with open operating systems which make addition of pirate software relatively easy, but the mobile telephone industry ecology mitigates against widespread sale of devices pre-loaded with pirate software while the set-top-box industry ecology actively supports it.)

International considerations

Q7: Please provide examples of where this issue has been raised with law enforcement agencies or government officials/ministers in other countries.

- ISD networks operating in the Eastern hemisphere came to CASBAA's attention in 2010-2011. The first networks were targeted at consumers of ethnic Asian programming – specifically Chinese programming. The users targeted by marketing campaigns for the boxes were usually located in developed markets such as the U.S., Europe and Australia.[2]

- TVB, the major broadcaster in Hong Kong and one of the world's largest exporters of Chinese-language TV content, began seeing substantial financial effects on its overseas businesses, as TVPad and other ISD syndicates sold boxes that provided "free programming" in competition with TVB's legitimate paid services in various countries.

---

the company's affiliates selling legitimate products banned from international trade shows, including last year's IBC exposition: http://www.digitaltveurope.net/597082/ibc-bans-gotech-as-nagra-wins-us-court-case/

[2] An example of a relatively large early entrant into the ISD business is the TVPad syndicate, headquartered in Shenzhen, China and offering pirated content to consumers in other countries. The activities of this syndicate were detailed in two court cases in the Central District of California, *(CCTV, TVB, and Dish Network vs. Create New Technology (HK) Ltd. et al,*and *Munhwa Broadcasting Corporation et al. vs. Create New Technology (HK) Co. Ltd et al.)*

Australia

- TVB was successful in persuading the Australian police to take a pro-enforcement stance. Police in the Sydney metropolitan area conducted raids in 2011 on retail premises where ISD boxes were being sold. These raids resulted in several arrests and seizures of box hardware[3].
    - Unfortunately the cases later had to be abandoned, and the pirate hardware returned, when prosecutors determined that Australian legal strictures were not adequate to produce convictions, despite the blatantly infringing nature of the content being delivered by the boxes in question.
    - This was the first of many indications that – despite the clear infringing purposes of the ISD activities – existing laws were inadequate to achieve any meaningful level of enforcement.

- The ISD industry developed rapidly, and boxes were soon appearing in Asian markets which offered not only Chinese programming, but large quantities of international programming, Hollywood movies, etc. (The markets initially targeted were those, like Singapore, Hong Kong, and capital cities in Thailand, Vietnam, Indonesia, etc. where broadband connectivity was most widely available.) Marketing campaigns began to appear which targeted speakers of languages other than Chinese.

- Sports content was soon added. Feeds of premium sporting events (in whatever language, but frequently English) available through ISDs substantially increased the marketability of the boxes.

Hong Kong

- Concerned about the effects of the expansion of the ISD industry, CASBAA organized a meeting of Hong Kong policymakers and enforcement agencies on September 4, 2012. In this meeting, industry representatives demonstrated the ease of plug-and-play operation of an ISD that was freely available in the shops of Hong Kong, along with the exceedingly wide range of VOD movies as well as linear channel streams available on the boxes.

- The government undertook to study the issue, but the initial results of that study concluded that Hong Kong laws, too, were inadequate to authorize any enforcement action, despite the blatant infringement. The authorities urged industry to support amendment of the Copyright Ordinance to make electronic communication of copyrighted content an offense. (The amendments were subsequently blocked in 2016 by the legislature, confounded by its neuralgia over intrusions into freedom of expression.)

[3] http://www.smh.com.au/technology/technology-news/police-raid-sydney-pirate-pay-tv-outfit-offering-1000-channels-for-90-a-month-20111213-1otn7.html

- Then, in June, 2014 Hong Kong pay-TV distributor PCCW Ltd. (d/b/a Now TV) was able to persuade the Customs police to use content uploading activities as the cause for an enforcement raid against an ISD syndicate operating the "Maige" box network. The raid found conspirators circumventing access controls on certain Now TV channels and streaming them into the Maige content servers (located overseas). Arrests were made at the upload site as well as at retail premises selling the Maige boxes, on the grounds that both sets of activities formed part of a single circumvention conspiracy.
    - These cases were the subject of considerable wrangling, as Customs and the prosecutors debated whether an adequate basis existed for prosecution under Hong Kong laws. After more than two years of deliberation, cases were finally lodged in late 2016, and a trial date is expected to be set soon.
    - While the industry has not yet been briefed on the nature of the charges laid, we believe that Hong Kong is attempting to follow the UK example, and pursue the arrested individuals for participation in a conspiracy under the common law.

USA/UK/Canada

- In 2014/2015, TVB lodged separate complaints with enforcement authorities in the USA, UK and Canada about the ISD problem, and requested criminal actions be taken to interdict the importation and sale of such boxes. The enforcement authorities expressed sympathy on the problem, but all responded that there was no usable provision in their laws to enable them to take such actions.

Singapore

- CASBAA and its members raised the problems of open ISD sales in Singapore with police and regulatory authorities on several occasions after 2011. On each occasion, the officials responded that they could not see a way under current laws to enforce against the boxes.
- In September 2013, CASBAA wrote to the CEO of the Media Development Authority of Singapore and to the head of the police Intellectual Property Rights Branch formally asking for action against open ISD sales in Singapore. The authorities did not respond.
- In September of 2015, CASBAA again wrote to the CEO of the Media Development Authority, providing evidence that open sales of fully-loaded ISDs were taking place in a major Singapore trade show. The letter observed that these particular ISDs offered consumers subscriptions to a TV service which, in addition to constituting blatant violations of the intellectual property rights of many content owners, was an unlicensed pay-TV service under Singapore's laws, and it asked the MDA to use its (ample) investigative powers to send a clear message about the unacceptability of such infringing unlicensed services. The Authority contented itself by asking if content owners would consider beginning civil copyright litigation against such boxes, and did not address the blatant illegality of such services under the Broadcasting Act.

India

- ISDs have not yet made much of an impact on India's domestic TV market – the result of weak broadband connectivity and low domestic content prices. However, Indian content companies complained to the Indian authorities in 2013 and 2014 about external ISD-based piracy of their content, which saw content streams originating in India being transmitted to external markets, depriving the content owners of legitimate overseas revenues as aggressive marketing of the ISDs to customers resulted in cancellation of many subscriptions to legitimate content suppliers.
- Indian enforcement authorities were responsive. The complaints and investigations by the content owners resulted in Asia's highest-profile enforcement action in June 2014, as a raid by police in Hyderabad resulted in breaking up the arm of a multinational syndicate that was operating an upload point for more than 100 TV channels. Four conspirators were arrested. (Appended here is a photo of broadcast media coverage of the high-profile arrests.)

USA, again

- In May, 2014, CASBAA briefed U.S. trade agencies in Washington on the burgeoning problems caused by ISD networks in Asia for US-based content providers. The Washington interlocutors were sympathetic, but noted that the legal framework was not well-suited to bringing action against importers or retailers of ISD boxes, which were utilizing unencrypted internet streams to deliver programming to consumers. They noted that the most clearly infringing activities (e.g. decrypting and uploading the content streams) were happening in other countries.

- CASBAA understands that following those meetings, and parallel representations by the US content industry, the USG began making China's role in the ISD industry a discussion point in bilateral intellectual property negotiations, as evidenced by the final statement of the US-China Joint Commission on Commerce and Trade, in November 2015, which included a paragraph on "*Enhanced Enforcement Against Media Boxes and Unauthorized Content Providers"*.

China

- CASBAA led a delegation of content providers to Beijing in September 2014, to brief the National Copyright Administration of China on the problem of ISD - based networks. (ISDs were at that time also being widely sold to Chinese consumers.) The delegation underlined the central role played by the Chinese hardware industry in making and promoting ISD boxes, as well as the fact that many of the ISD syndicates seemed to be headquartered in China. The Chinese officials expressed interest in taking enforcement action against any syndicates delivering unauthorized content to people within China, but noted that under Chinese copyright law, delivery of infringing content to consumers outside China was not a crime.
    - In mid-2015 the Chinese State Administration for Press, Publications, Radio, Film and Television (SAPPRFT) promulgated regulations to control production and sale of ISDs. According to the regulations, set-top boxes could only be legally manufactured if their software "locked" them to streams provided by licensed Chinese content suppliers, and they could not have USB ports or other means by which third-party software could be loaded on the box. These measures had a pronounced effect on the ISD industry within China (curtailing it, and driving it more underground), but in keeping with China's territorial approach to these issues, no restrictions were placed on manufacture of boxes for export to other jurisdictions.

All of these examples testify to the difficulty of obtaining effective enforcement against mass infringement networks under existing legal frameworks. Government after government has admitted there is a serious problem, which cannot be efficiently addressed under current laws. The ISD syndicates operate transnational content delivery systems, and they are adroit in delivering infringing content to sap markets in countries with otherwise-good IP environments, while using non-cooperative jurisdictions, gaps in national laws and internet obfuscation to shield themselves from enforcement.

CASBAA's view is that no country has copyright laws that are sufficiently well-tooled to repress these activities. Achieving a meaningful level of enforcement will require bringing to bear the same law enforcement tools which are used against other transnational conspiracies. We would urge governments to:

-- Improve copyright laws to ensure seamless coverage of international content transmission – an infringement conspiracy should not be able to hide behind facile distinctions like "downloading is illegal, but streaming is not."

-- End the exclusive territorial focus of copyright enforcement (see Q9 below for how this recommendation might be implemented in the Singapore context, as an example)
-- Use other laws (e.g. those against common frauds and conspiracies, or those requiring broadcast licensing) to repress the activities of transnational infringement conspiracies, i.e. the ISD syndicates.
-- Implement laws and regulations to deny the conspiracies access to illicit revenues through subscription transactions as well as ad sales.
-- Require the internet industry to achieve a meaningful level of self-regulation, supplemented if necessary by external regulatory and legal constraints, to achieve a situation where legitimate firms no longer support and promote illicit activities, including through activities like site hosting and online search. "Know your customer" should become the watchword for internet service providers.

Q9: Are there examples of enforcement powers in other countries that have been introduced to deal with these issues? Please provide examples of approaches you are aware of in other countries and any evidence you have of their success.

As may be clear from the preceding discussion, we do not believe that the legal situation with respect to ISD-based infringement is satisfactory. Candidly, the answer to this question is "no, there are no examples of success in Asia." Indeed, in our conversations with Asian leaders, we now regularly point to the energy and ingenuity of the UK enforcers as a global "best practice." Imitation is the sincerest form of flattery, and in that regard we note that the Indians have already emulated PIPCU by establishing a dedicated enforcement unit in Telangana state (TIPCU) and it was recently announced that the state of Maharashtra will soon follow suit and establish a MIPCU[4]. We hope that some Asian governments will also emulate the legal approaches being explored by UK police authorities, such as pursuing the ISD retailers and operators under conspiracy laws.

We also consistently point out to Asian governments that part of the duty of a regulator is to maintain a healthy industry ecosystem, and to that end they should not ignore violations of their broadcasting laws or other laws, committed by ISD syndicates (as in the case of the Singapore subscription piracy network mentioned above.) Sadly, IP protection is too often regarded as only the job of intellectual property offices, leaving industry regulators free to concentrate on more agreeable duties.

We are also pressing for improvement in the laws. Most recently, we engaged an eminent Singapore IP lawyer to advise on possible changes in that country's copyright law which could result in an improved environment for IP enforcement, and we made a submission to the Singapore Ministry of Law as part of an ongoing copyright review, to seek such changes. Among the key changes we sought would be:

- **"Streaming:** Provisions in the Copyright Act that refer to copying/reproduction should be updated to also extend to streaming/communication of the work, given that the

[4] http://www.indiantelevision.com/specials/event-coverage/ficci-frames/ficci-frames-17-maharashtra-to-form-ip-crime-unit-to-fight-online-piracy-170322

streaming facilitated by the ISDs may not be considered to be a reproduction per se, but it causes every bit as much damage to rights owners as reproduction and sale of a physical copy. For example, section 83(a) of the Copyright Act provides that making a copy of a film is one of the exclusive rights in relation to a cinematograph film, but streaming of films would not be found to fall foul of this section since no local copy of the recorded programme is kept when content is streamed.

- **"Circumvention conspiracies**: As noted above, the ISDs on sale in Singapore are the retail end of an international conspiracy. The key activity of the conspiracy is circumventing protection measures for pay-TV program streams overseas (e.g. in China), and replicating those streams on the internet. The retail operations in Singapore and elsewhere generate the revenues and profits. Currently, the anti-circumvention provisions in Part XIIIA of the Copyright Act do not apply to acts of circumvention that occur outside of Singapore, so we propose updating this section to extend to circumvention that occurs outside Singapore, where the material that was protected by the anti-circumvention measure is subsequently made available in Singapore through the ISD.

- **"Infringing Articles:** Section 136 of the Copyright Act should be updated, such that an "article" which allows unauthorized communication of the work should be considered as an infringing article. (Currently, S136 only makes reference to "infringing copy."

- **"Prosecutorial discretion:** We also propose amending S136 to provide for the flexibility of drawing up charges on the basis of articles seized or infringing copies/streams. (Typically, the articles seized are considered based on the physical articles seized – the medium of storage.) At the point of enacting s136, one infringing copy of a cinematographic film would typically reside in one optical disc. Today, many cinematographic films can be stored in a single storage disc, and a single ISD can give unauthorized access to thousands of programs/films. More flexibility in s136 would allow for a more proportionate exercise of prosecutorial discretion.

- **"Locus Standi**: Currently, only copyright owners or exclusive licensees can sue for infringement; for the anti-circumvention provisions, S261C(2) of the Copyright Act provides that only the copyright owner is allowed to take action in relation to any contravention. This approach is unnecessarily restrictive and we propose that non-exclusive licensees should also be able to take action against infringers/circumvention, as long as they do so with the consent of the copyright owner. This would make it easier for local industry players who may be non-exclusive licensees to protect the local market. (We note that – partially as a result of the MDA's "cross-carriage" policy that deters signature of exclusive distribution agreements – there are exceedingly few exclusive channel distribution licenses in today's Singapore television industry.)"

We share these details in the knowledge that the changes proposed may not be relevant to the body of UK law, but so that the reader can see the types of improvements that we believe are a necessary start to improving Asian copyright laws. (The entire text of our submission in the

Singapore proceeding can be found at http://www.casbaa.com/regulatory/casbaa-submission-on-ministry-of-lawws-proposed-changes-to-singapores-copyright-regime/.)

Once again, we thank the IPO for seeking industry views on these important questions. We will be happy to provide additional information if desired, and we look forward to continued dialogue with the IPO going forward.