Illicit IPTV Streaming Devices – Call for Views: Motion Picture Association response

Summary

The Motion Picture Association (MPA) welcomes the opportunity to respond to this call for views. The use of "plug in" media players (referred to from here on as 'devices') to facilitate online copyright infringement represents the fastest growing challenge to effective copyright enforcement, which is fundamental to generating growth and innovation in the global audio visual industry (including film, television, sport, music and other audio visual content).

Addressing this issue requires a comprehensive strategy, namely one that deals with each component of this serious problem:

- the relevant apps and add-ons, as well as the entities and individuals who create, exploit and host the apps and platforms that facilitate access to the infringing content;
- the applicable hardware devices, as well as the entities and individuals who import, load, advertise, market and sell devices; and
- the entities and individuals who host and promote services where the infringing content may be accessed.

It is also important to note that where, currently, consumers may **have** to acquire physical devices and/or load up specific platform or other software in order to access the content via a television set, fast-developing innovation will result soon (or has resulted already) in it being possible to access the content directly from e.g. a TV set in a consumer's living room – as long as that TV is connected to the internet.[1]

Furthermore, the global nature of this phenomenon presents additional issues – for example:

- consumers in multiple non-UK markets are accessing (free of charge, or at reduced fees) services such as the UK (or other major market) Premier League and other sports offerings;
- UK consumers are accessing content such as US NFL broadcasts, releases of films and TV content that has not yet been released in the UK (that may be pending for release or still showing in UK cinemas);
- children and young people in the UK cannot be protected from age-inappropriate advertising or content.

Effectively tackling this issue presents a number of challenges and it will require action in several different areas. This should include, but not be limited to, legislative changes.

The key points outlined in this submission and an associated annex are as follows:

- There is a gap in the current legal framework that makes it challenging to secure successful prosecutions against the key individuals involved in facilitating the configuration and spread of these devices. This includes those involved in marketing, selling, distribution and delivery as well as those supporting the sources of content, the platforms facilitating it and the software that connects the sources of content with the individual devices;

[1] It should also be noted that the activities described here may be conducted on laptops, tablets, mobile devices etc. as long as the applicable platform software and "add-ons" are installed there.

- Addressing these gaps in the legal framework requires new legislation via a new clause in the Copyright Designs and Patents Act 1988;
- There are significant technical challenges when gathering evidence and undertaking enforcement actions in this area both due to the complex technical nature of the devices and associated services and also the international nature of the networks and infrastructure that support them;
- Therefore a nationally and internationally coordinated approach between law enforcement, the IPO and industry are paramount to tackle these challenges effectively. To provide for such effective cooperation, it is important to ensure key enforcement organisations such as the Police Intellectual Property Crime Unit and local Trading Standards bodies have sufficient resources and information to work with industry to address this issue.

The nature of the challenge

Overview

The Consultation Document correctly identifies that one of the key elements of this issue is the increasing use of (often small) plug and play media devices (such as set top boxes (STB) or USB sticks) onto which add-ons or apps have been installed (so-called 'fully loaded devices') that facilitate online copyright infringement via consumers' main television set.

However, it is also important to understand that the larger issue not only concerns the devices (which fall into different categories in terms the nature of their operation, the content they provide and how they are distributed to consumers), but also the platform software that facilitates the activity as well as the apps and add-ons that leverage the platform and facilitates access to the infringing material.

An initial step, in the form of new legislation to deal with 'fully loaded devices', will be very important. However, this issue will require ongoing attention and, likely, innovation, dialogue and collaboration between rights holders, government, law enforcement, retailers and others in order to address other components of the eco-system and to educate consumers.

With Regard to Hardware Devices (*Boxes and Sticks*):

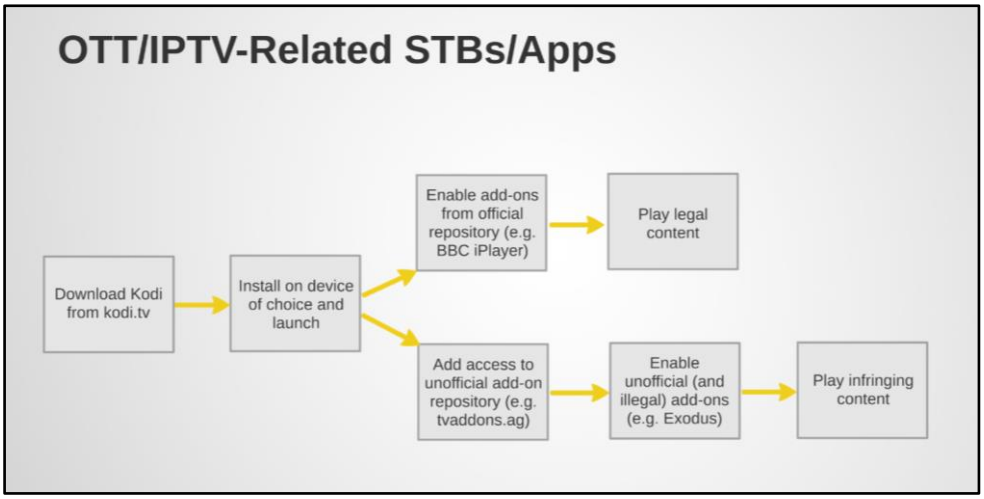
These hardware devices can be purchased incorporating professionally pre-loaded platform and content-accessing software. Alternatively they may be purchased blank, but "packaged" with instructions for incorporating illegal third party plugins or add-ons and then configured using the instructions. There are also devices that are in use already for authorised purposes which may be altered (often requiring that the device is "hacked") using instructions found easily online at YouTube.com and other services. Once loaded up with the necessary platform software and add-ons, these types of devices provide unauthorised access to thousands of streams, or other infringing sources, of television, film, sport, music and other content available online.

Though the devices cover a number of different types of service these generally fall into two categories (though these categories are not mutually exclusive and both can sometimes be delivered through the same device):

1. **Illegal 'OTT subscription services'** that transmit live entire TV channels (usually with time shifting options) and often against payment of a subscription fee. The user can obtain a subscription (together with the required device and software) directly from the illegal service provider (or their reseller).

2. '**Fully loaded' service providers**: these typically relate to devices (set top boxes or USB sticks) that have been loaded with, or come with simple instructions to load, illicit software add-ons or apps (or sometimes are sold in their unaltered, 'vanilla' state but with clear indication in their marketing that they can be used / are intended to be used to access infringing content).

Below is an overview how a pre-loaded device can be configured to provide access to illegal content. As mentioned above, there has been a significant increase in individuals selling these devices pre-loaded or blank with instructions for incorporating these illegal third party add-ons or apps.



Sellers offering these types of fully loaded devices and services are currently easily found on mainstream marketplaces such as Amazon, eBay and Facebook (though Amazon has recently announced a new policy to crack down on these devices – more detail below[2]).

Both types of service provide unauthorised access to thousands of streams of television, film, sport and other content available online and are very damaging to rights holders.

These variations are outlined in more detail below. They are all facilitating copyright infringement on a mass scale but they present different challenges that need to be considered from an enforcement perspective.

The consumer perspective

Widespread availability on reputable online market places such as Amazon and eBay, along with increased peer recommendations have helped to create a perception of social acceptability for these devices and sown confusion about their legality; 33 per cent of UK owners of such devices admit to not knowing whether the devices are legal or not and these users tend towards an older demographic than observed for other forms of piracy.[3] These factors together with low prices have facilitated their rapid spread. Some of the devices can be purchased for as little as £20 to £50 depending on the model

[2] Amazon policy: https://www.amazon.com/gp/help/customer/display.html/?&nodeId=200277240
[3] Industry Trust report: *IPTV Piracy: A study on set-top-box and stick infringement for the industry*

and this is reflected in the fact that nearly a quarter (23%) of owners of such devices in the UK say they received their device as a gift (often from a family member).[4]

From a technical perspective, the level of technical knowledge required to access infringing content is minimal; these devices will either come 'fully loaded' with the software and add-ons required to access the infringing content or with easy to follow instructions about how to configure the device to facilitate access to what are infringing sources (this is intended to insulate the providers of these services from liability). Installation guides can also be found easily online, at YouTube.com and other services and in some cases the devices are sold in their un-altered format without instructions but the associated marketing either implies or makes clear that they are intended to be, or have the potential to be used to access infringing content.

The devices also help to socialise the act of accessing this infringing content by making it available on the main television set. More than half (54%) of parents surveyed reported watching infringing content through their set-top box or stick with children aged under 18 in their household, while one in five (20%) of 11-15-year-olds have engaged in IPTV piracy.[5]

These devices also raise a number of issues relating to child safety and the availability of age inappropriate content due to a lack of content filters or an increased level of complexity in applying them. Furthermore, infringing content online generally does not comply with relevant regulation. These issues have been highlighted in a letter to the Secretary of State from the Children's Charities Coalition on Internet Safety, a group representing 10 leading UK children's charities.

The landscape of IPTV piracy

It is important to understand that the individual devices themselves are just the end-point of a complicated commercially-driven eco-system that facilitates access to infringing material in this manner.

A basic overview of some of the key elements that support this eco-system is as follows, though it is important to note that the way in which these operate and are maintained differ across the different variations of services available.

The devices (boxes and sticks) are manufactured and imported – often on a large scale from China – albeit the devices are in their 'vanilla' or unaltered state.

These devices can then subsequently serve for illicit use by **OTT subscription services** or fully-loaded service providers.

OTT subscription services configure the devices so that their subscribers have access to the illicit TV channels. The devices are configured so that they provide the user with access to the servers where the illicit content is streamed from and where metadata and users' access authentication is provided.

When content is accessed on the device it essentially performs a three step function in order to access content, each step of which provides a potential point of disruption for the applications.

[4] Ibid
[5] Ibid

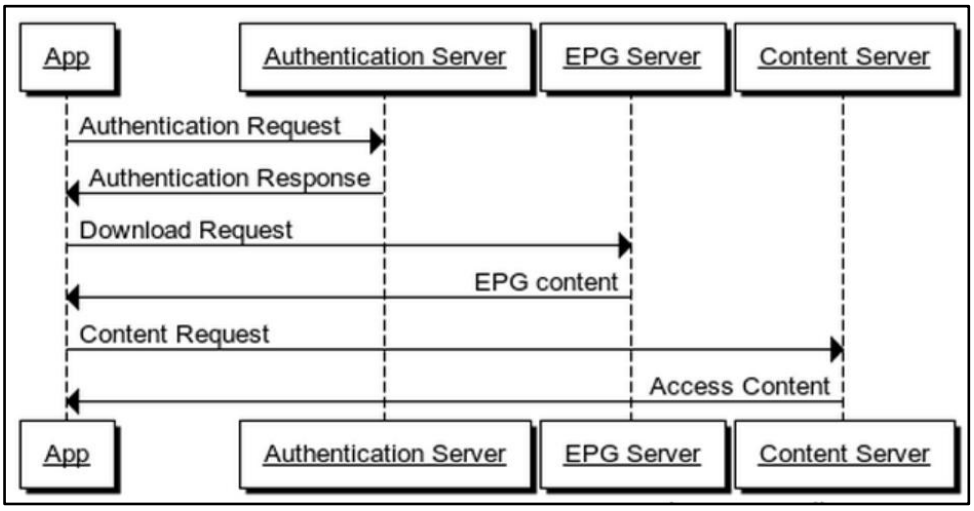


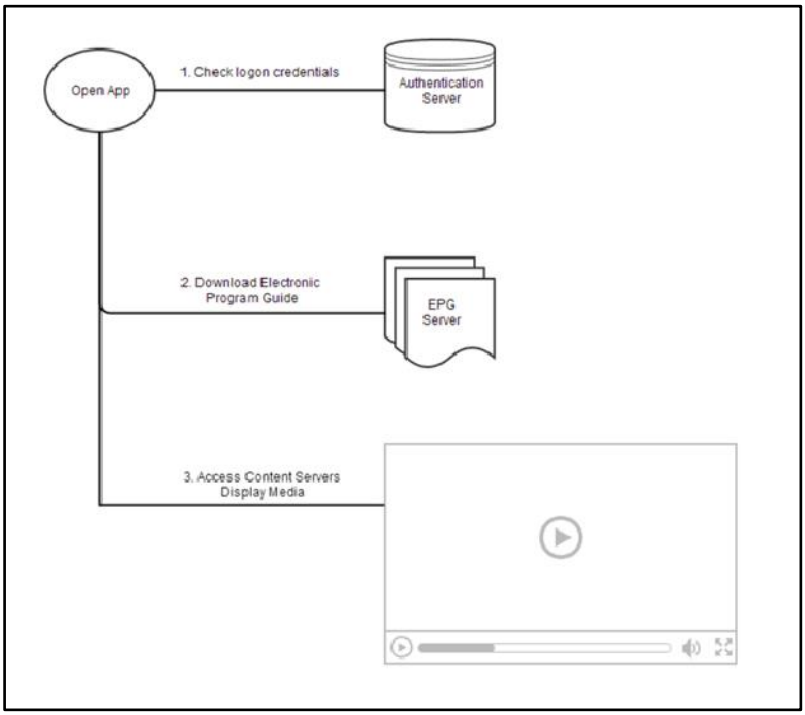
Image: Sequence Flow of Accessing Content

In order to access content, the following process is performed:

1. Authentication request
2. Access the Electronic Program Guide (EPG)
3. Access Content (Stream or Hosted)

In the first stage, authentication takes place against the authentication server. Failure to authenticate means the user cannot progress any further and access infringing content.

Once the user has successfully authenticated with the server, a request is made to access an EPG, which essentially provides links to content. If the EPG is unavailable, access to content is inhibited as the content does not exist on the site/app directly, and no accessible links renders the IPTV service useless. When the users click on a link, the app then sends a request to access content from the content server.



The content servers (also called 'Content Delivery Network' or CDNs), servers relating to the Electronic Programme Guide ("EPG"), as well as Authentication servers are often located in physically different places and managed by third parties.

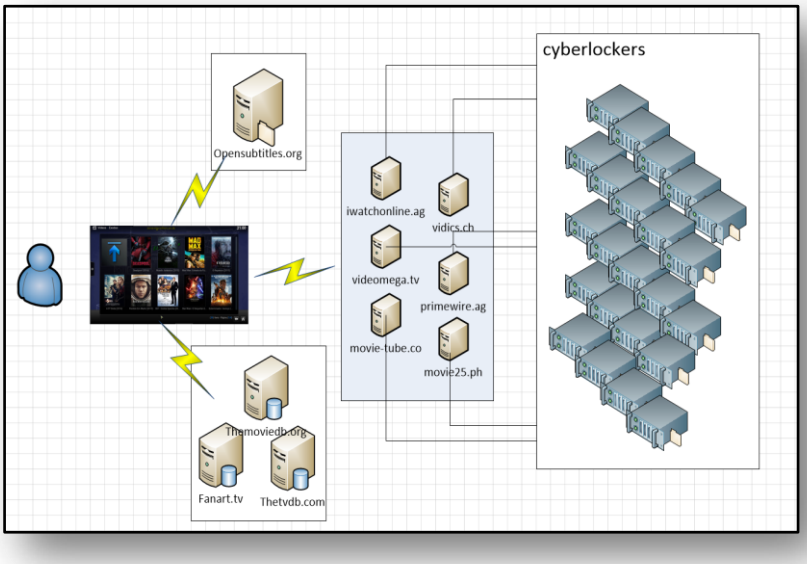
Moreover the infringing content can be delivered via internationally dispersed content delivery networks.

Generally subscriptions can be purchased directly from the main provider or through a network of local resellers.

On the other hand, **fully loaded service providers** make devices available either 'fully loaded' or with instructions on how to activate the infringing element of them, or in some instances simply sell the unaltered boxes while making it clear in associated marketing that it has the potential to be used to access infringing content. The add-ons and apps that are installed on these devices are developed and maintained by yet other individuals that easily hide behind online aliases.

Similarly to apps that can be downloaded from app stores, add-ons are downloaded from online 'repositories'. Repositories are basically online servers (operated by the add-ons developer itself or a third party) on which the source code for the add-ons are stored.

These unauthorised apps and add-ons 'scrape' content from linking and streaming sites – who aggregated all the links from sources such as cyberlockers – to download and stream infringing film, TV and sports content, as well as subtitles.



The devices are distributed through a variety of distribution channels including mainstream online retailers such as Amazon and eBay (again, for more detail on Amazon's recent policy change see below).

For both types of service payment processing services such as PayPal are frequently used by the individuals involved in distributing the devices.

This complex picture is made still more challenging from an enforcement perspective due to the geographically distributed nature of each of the components of these services. Everything from the device importation, development of illegal 'add-ons' and location of the servers through to the individuals configuring, marketing and distributing the devices, the location of the online retailers and payment processing services can be, and often are, all spread across multiple countries.

Rights holders are already working, along with law enforcement, to identify ways of disrupting this activity by targeting individuals and entities throughout this eco-system – for example, discussions are ongoing with the online retailers. One positive recent development was the adoption of a new policy by Amazon prohibiting the sale of illicit devices on its marketplace with the threat that the inventories of third party sellers may be destroyed without compensation if they do not comply.[6] This policy was only announced very recently and we will monitor its impact closely and will continue our dialogue with online retailers.

This is a complex picture and much of this activity is still a work in progress. Some of these approaches are set out below in more detail alongside recommendations for how the UK Intellectual Property Office (IPO) and UK Government can support these efforts. However, it is important to understand that the gaps in the legal framework are hampering the ability to make progress on this issue as quickly as required and need to be addressed urgently.

In the sections below, we have addressed the questions set out in the consultation but we note that these questions do not fully address the scope of this issue. As indicated above the eco-system of

[6] Amazon policy: https://www.amazon.com/gp/help/customer/display.html/?&nodeId=200277240

these services relies on many different parties that each play a significant role in providing access to the illicit content individually (such as infringing linking, streaming websites) or when offering access to illicit content through a combination of technologies (such as sellers of fully loaded devices on which add-ons are installed with the sole purpose of providing access to infringing linking or streaming websites).

Scale of the problem

Q1: Please provide evidence of the scale of the problem of illicit IPTV streaming devices and the economic harm it is causing to broadcasters and content owners.

Consumer research conducted by ICM estimated that 19% of adults admit to engaging in IPTV piracy, with nearly half starting to participate in just the last 12 months. As a point of comparison, engagement with other, longer-standing forms of digital piracy via laptops and smartphones stands at 23% at present.[7]

UK Google Search behaviour also supports the rapid rise of set-top-box and stick infringement, revealing a 143% increase in associated searches between November 2015 and November 2016 – a more advanced upward trajectory than for global searches. Furthermore, a quarter of UK adults expressed intent to buy a set-top box or stick as a Christmas gift in 2016, with one in ten expecting to use it to watch copyright infringing content.[8]

Research from ICM has found that IPTV Piracy is already having a direct impact on consumer spending. Two in five (41%) of those engaging in IPTV piracy say they spend less money on going to the cinema as a result of their access to pirated films, compared to 22% who engage in other forms of piracy. This trend is even more pronounced for disc purchase and subscriptions.[9]

The potential impact of IPTV Piracy on sports subscription services is also significant, with the opportunity to watch live sport for free cited as a particular draw for younger men. Of the 19% of infringers using IPTV Piracy, nearly two thirds (62%) reported using IPTV devices to watch live sports at least once, with 11% admitting to doing so more than once a week.[10]

These findings are mirrored by the scale of activity on one of the main repositories of infringing add-ons for Kodi – called TVAddons.ag. According to their own figures, the number of unique users doubled from December 2015 to October 2016 to a rough average of 5.6 million per day and 24.7 million a month.[11]

To put these figures in context, Netflix has 80 million paid subscribers worldwide, Spotify has 40 million paid users, and Sky 22 million.

In addition, video tutorials are widely available on YouTube that explain how to install infringing Kodi add-ons and how to use them to watch infringing content.

[7] Ibid
[8] Ibid
[9] Ibid
[10] Ibid
[11] Torrent Freak: Pirate Kodi Add-Ons Gain Massive Popularity: https://torrentfreak.com/pirate-kodi-add-ons-gain-massive-popularity-161007/

The scale of the problem is already significant but of most concern is the fact that this activity is increasing quickly, while the legal and enforcement mechanisms needed to properly address it often require significant time and resource to deploy.

Q2: Please provide examples of cases that you are aware of (with references where possible) where prosecution in the UK has been successful for the:

- ***a. Import;***
- ***b. Offer;***
- ***c. Sale; or***
- ***d. Use of set-top boxes for illicit streaming.***

Please indicate the legal basis used for these prosecutions.

A. Import: Trading Standards Scotland had the first known conviction in the UK. Case v Gavin Gray- This was a card sharing investigation where Gray was selling access to sports channels and was supplying Mag250 boxes. This investigation revealed £13 million pounds of sales connected to China. Gray was recently convicted.

B. Sale of: Moreover Gray advertised his criminal business on dedicated card sharing websites and forums, supplying unlawful access to homes across Scotland.

When officers searched his home in Mossend, Belshill, they seized £44,500 hidden in a safe in the loft. Police were also able to later seize £80,000 from his bank account.

Gavin Gray was sentenced on Monday 6th March 2017 at Hamilton Sheriff Court after pleading guilty to four charges of fraud and offences under the Copyright Designs Patents Act 1988. Specifically he was found to have breached sections: 297A(1); 296 ZB(2); 296 ZB(1)(c)(iv) of the Copyright Designs Patents Act 1988.

Q3: Please provide examples of cases you are aware of where prosecution of ostensibly valid cases was not pursued under the above provisions. Please indicate why these cases were not taken forward.

In light of ongoing investigations we cannot name the targets or provide concrete examples. However, upon request we can confidentially provide examples where, despite services affecting UK rightsholders, it appeared not possible to bring a criminal prosecution in the UK. This is mainly due to the internationally dispersed nature of the case.

Efficacy of existing legal framework

Q4: Are there specific areas where you believe the current legal framework does not provide the necessary tools to investigate and prosecute this issue? If so, please provide as much detail as you can on how you think the current provisions could be amended and how these amendments would address the perceived gap.

Q5: Is there any UK case law which you believe limits the applicability of the statutory offences listed above?

We feel it is best to address questions 4 and 5 in tandem. MPA's view is that the existing legal framework does not provide the tools required by rights holders to tackle IPTV piracy through criminal enforcement. Legislative amendment is therefore vital. Given the strategically sensitive nature of some of the points raised, we have provided our substantive answer to these questions in a separate annex.

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.

Regardless of the offence used to try and tackle these devices, there are a number of challenges, particularly from a technological standpoint, in gathering evidence to support cases. Given the strategically sensitive nature of some of the points raised, we have provided our substantive answer to this question in a separate annex.

International considerations

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

The fact that the spread of these devices at scale is still relatively new means most law enforcement agencies and governments are at an early stage of trying to tackle them. However, there are some interesting examples where cases have been successfully brought to conclusion. Given the strategically sensitive nature of some of the points raised, we have provided our substantive answer to this question in a separate annex.

Q8: Please provide examples of where there is an international element to the supply and support of this activity in the UK, and give your views on how this dimension of the problem could be addressed in terms of: a. The supply of illegal boxes; b. Websites hosting illegal content; and c. Other illicit streaming services.

Given the strategically sensitive nature of some of the points raised, we have provided our substantive answer to this question in a separate annex.

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.

N/A

Other barriers to prosecution (resource, jurisdiction)

Q10: Are there any other barriers to the successful investigation and prosecution of these issues?

In addition to addressing the gaps in the legal framework, it is important to ensure sufficient resources are secured for key enforcement organisations. In particular, the Police Intellectual Property Crime Unit (PICPU) will have a key role to play and it is important it has the resources it needs.

PIPCU deploys a number of tactics to achieve this including bringing cases against those running services that facilitate copyright infringement on a major scale and is seeking to target those that play a key role in the digital TV piracy ecosystem. However experience from across the audio-visual sector is that PIPCU is overstretched, leading to significant delays in prosecutions in relation to the making available of illicit streaming devices, notwithstanding PIPCU's and its staff's strong commitment.

Furthermore as the components that are responsible for the working of these services are often dispersed over different countries, it should be ensured that PIPCU has the appropriate means to obtain international cooperation from other national and international law enforcement bodies and foreign industry stakeholders.

PIPCU is recognised as an effective body across the creative industries and must be provided with sufficient resources to effectively protect UK rights holders. However, it is important that PIPCU remains, and is seen to remain, operationally independent and should continue to receive its core funding from the Government. It is vital that the Government secures PIPCU's funding for the long term, as its current funding is not guaranteed beyond 2017. This funding settlement should in particular ensure PIPCU is able to devote additional resources to the issue of digital TV piracy.

Local Trading Standards organisations can also have a role to play in addressing this issue and it is important, at the least, that they are properly educated about the illegal nature of these illicit devices and the infringing services they facilitate. It is important that they understand that these services are illegal and communicate this to the local communities in which they operate. The IPO should play a role in ensuring Trading Standards organisations are properly educated on this issue.

Q11: Do enforcement agencies have the powers required to investigate this activity? Given the split in offences between IP legislation and other provisions such as the Fraud Act, are warrants readily available to those investigating?

N/A

Q12: Are there specific areas where further guidance (from IPO and/or CPS) would be beneficial in the investigation and/or prosecution of this activity?

The Intellectual Property Office (IPO) produces excellent reports and documents to support investigations. They also have excellent relations with PayPal providing law enforcement with the tools to prosecute offenders and thus it is hugely beneficial to involve the IPO in investigations and prosecutions at national level across the whole of the UK.

The challenges are largely related to the gaps in the legal framework and technical evidence gathering process outlined above.

Other suggestions comments

Q13: Are there any non-legislative approaches that you think could help with the situation? Please provide examples.

Ultimately, as with the strategy to tackle online copyright infringement on a wider scale, a number of different strands will be required that target different aspects of the IPTV piracy eco-system. Some of these will be taken forward on a non-legislative basis. For example, as outlined above, rights holders are already engaged in discussions with major online retailers on this problem, with the recent new

policy at Amazon a welcome development, and we expect this dialogue to continue. Rights holders are actively exploring options to target the various parts of the eco-system from a technical perspective.

Rights holders have attempted to use requests for content to be taken down from social media sites to combat this issue. However, the ease with which individuals involved in marketing and distributing these devices are able to constantly change names and online profiles on social media platforms has severely limited the effectiveness of this approach.

However, it will still be vital to target the individuals that are key to the marketing and distribution of the devices in the UK. In order to do this effectively it is critical to address the gaps in the existing legal framework in order to make significant progress in addressing this issue. As outlined above, MPA believes that primary legislation will be needed in order to achieve this.

Furthermore, as mentioned above, it is critical to continue to work with retailers to address the promotion and sale of these devices via their marketplaces, as well as to work with social media companies to address discussion around and promotion of the devices and activities - and to educate consumers.

Finally, we believe the IPO has recognised already the need for clarified guidance about existing legislation and training on the specific issue of IPTV piracy for Trading Standards Officers and we hope that this will be accomplished as soon as possible. It would also be helpful for the IPO to ensure that there is clear guidance on this matter for consumers – as some recent media coverage (especially that quoting statements from Derbyshire Trading Standards Office) has not been accurate or helpful.

Q14: Do you have any other suggestions or experience relevant to this exercise?

The general public do not appear to recognise the criminality involved in these products. Industry is already examining ways to incorporate messaging on this issue in existing education and awareness raising activity. The *Get it Right* campaign reminds people that they have a choice regarding the source and type of content they access and that their choice has consequences. Additional resource for this campaign would enable it to address issues relating to IPTV piracy more directly and we are keen to continue to work in partnership with the IPO and Government to deliver education campaigns such as this.

Finally, it will be important to monitor how the fundamental technologies and eco-systems that underpin IPTV piracy develop and take advantage of new technologies and consumer habits, such as increased uptake of smart TVs. It will be important for industry and Government to work together to identify and react to new trends as they develop.