IPO Call for Views: Illicit IPTV Streaming Devices

Sky is the United Kingdom's leading pay television service provider[1]. It is both a broadcaster and a retailer of content – in the latter capacity it retails its own broadcast channels and those of third parties. It also wholesales its own channels to a number of distribution partners, including Virgin Media, TalkTalk and BT, who in turn sell those channels to consumers as part of their own pay TV services. Sky currently employs over 25,000 people in the United Kingdom. Based on an Oxford Economics Report in 2016[2] Sky was estimated to support 94,200 jobs in the United Kingdom in 2016 and Sky and its employees contributed a total of £2.2 billion to HM Treasury in tax receipts in that period.

Sky observes, and is deeply concerned about, the growing scale of Internet Protocol TV (IPTV) piracy, which is the fastest developing area of intellectual property theft in the UK and beyond. A number of features of the Digital Economy have contributed to this including higher broadband speeds and the greater availability of bandwidth, which have enabled the unlawful redistribution of television broadcasts to both commercial and domestic users. IPTV streaming devices provide an easy way of illicitly viewing these retransmissions, depriving rightsholders of revenues that support investment in the underlying content.

In our response to the Intellectual Property Office (IPO)'s Call for Views, we set out the scale of the problem and why existing enforcement tools are ill-adapted to the specificities of the supply and use of IPTV devices to gain access to pirated digital content. Despite the widespread supply of illicit IPTV devices, and our extensive collaboration with law enforcement agencies, we are only aware of three convictions of suppliers of these devices in English Courts and a further, isolated, conviction in Scotland. These statistics alone strongly support the notion that the current legislative toolkit is inadequate and highlight the need for a bespoke offence.

In Sky's view, consistent with its submissions to the IPO over a number of months, legislation is needed and it should take the form of a specific amendment to the Copyright, Designs and Patent Act 1988 (CDPA) which criminalises the supply of devices or software intended to facilitate copyright infringement. The specific amendment we propose, together with the rationale for it, is set out in answer to question 4 below.

We are disappointed, having identified the problem in the Government's Intellectual Property Enforcement Strategy launched in May 2016, that the Government did not to seek to resolve it in the Digital Economy Bill that has been before Parliament for the last 8 months. We hope that the IPO's Call for Views will lead to the expedited introduction of new legislation.

The widespread availability of illicit streaming devices, if left unchecked, will have an adverse impact on the Creative Industries. Thirty organisations across a broad spectrum of industry recently wrote a letter to the IP

---

1 Sky also provides pay-tv services in four other EU member states, namely the Republic of Ireland, Germany, Austria and Italy.

2 Oxford Economics, The Economic Impact of Sky in the UK, 2016.

Minister calling him to update legislation to deal with the threat[3]. If intellectual property cannot be properly protected, the value of the underlying content will be undermined, leading to reductions in investment, and loss of jobs in this vital sector. These concerns were shared by many MPs and Members of the Lords during the Committee stages of the Digital Economy Bill 2016-17[4], with cross-party support for legislative changes in this area.

There is also significant concern that, absent clarity that this new type of piracy is illegal, there is an increasing perceived legitimacy to its use. This is leading to a 'normalisation' of copyright infringement particularly amongst the younger generation. Evidence suggests that users are four times as likely to perceive accessing infringing content through a device as legitimate (31%) compared to infringing content accessed via websites or torrents (8%)[5]. Furthermore, IPTV piracy typically takes place on the main family TV screen. This poses an additional threat to young viewers, who are being exposed to inappropriate content and/or advertising, as none of the usual broadcast protections are in place.

Whilst we believe updating legislation is an important element in combatting IPTV piracy, it is not the only change needed in order to clamp down on IPTV piracy. Effective enforcement is also important, to which end we call on Government to ensure proper and sustainable funding of enforcement agencies, most notably the Police Intellectual Property Crime Unit (PIPCU). Educational campaigns are also important, and we welcome the Government's support of campaigns such as GetItRight. In addition, we are concerned that the reporting of IPTV piracy in mainstream media lends legitimacy to that activity, which has been exacerbated by various comments and statements from Trading Standards in mainstream media. It is important that the record is set straight through clear and consistent communications that both the *supply* of illicit boxes and the *viewing* of illicit streams are unauthorised and constitute offences.

It will also be important that information society providers act responsibly in helping the Creative Industries fight digital piracy. We welcome the recent court decision requiring the UK's main internet service providers to block access to live streams of unauthorised Premier League football.

We believe that other companies in the internet value chain such as online marketplaces, search engines, app stores and social media platforms, all have an important role to play in combating this phenomenon.

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.

[3] Joint industry Letter to IP Minister 8 March 2017

[4] http://services.parliament.uk/bills/2016-17/digitaleconomy.html

[5] RedBlue study performed on behalf of Sky

We are aware of a number of studies and research that have been undertaken into illicit streaming and into IPTV piracy. The IP Crime report 2015/16 notes the increase in illegal TV downloads, and identifies one of the main challenges as being "set-top-boxes and the proliferation of IPTV, which offer viewers increasingly easy access to pirated digital content."[6]

The Industry Trust for IP awareness recently conducted a study on set-top-box and stick infringement[7] that comprised three waves between October and December 2016. This provides a robust evidence base that highlights consumer attitudes towards IPTV piracy. It also validates the rapidly growing scale of this phenomenon, notably:

(i) 19% of those surveyed in December 2016 admitted to engaging in IPTV piracy, with nearly half starting to participate in this form of piracy in the last 12 months. This figure shows a dramatic increase from the 14% who admitted in engaging in October 2016.

(ii) The majority of households (79%) using illicit IPTV set top boxes or sticks are using them on their main TV set.

(iii) One in five of 11 to 15 year olds have engaged in IPTV piracy, and more than three quarters (79%) of parents report that their children watch infringing content on their own with 7% of parents having installed illicit devices in their child's bedroom.

(iv) Nearly two thirds of infringers (62%) reported using streaming devices to watch live sports, with 11% admitting to doing so more than once a week.

(v) One in five of those infringing reported to be spending less on or to have cancelled altogether paid-for subscription services as a result of their behaviour.

The Industry Trust study further found that IPTV boxes and sticks are widely available with nearly 14,000 listings across 51 online marketplaces, equating to more than 4 million items in stock globally. The fact that IPTV devices are being sold on mainstream marketplaces adds to confusion and legitimises illicit streaming. For example, 48% of people agreed that if you buy a set-top box of stick from a retailer like Amazon, it must be legal. Amazon's recent change of policy to expressly prohibit streaming devices that "promote, suggest the facilitation of, or actively enable the infringement of or unauthorized access to digital media or other protected content" is a positive development reflecting the extent and severity of the problem. That policy change has resulted in a significant reduction in the number of devices listed on that market-place, but to date other market-places have not followed

---

6 IP Crime Report 2015-16, p.13: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/557539/ip-crime-report-2015-16.pdf

7 IPTV Piracy: A study on set-top-box and stick infringement for the industry by the Industry Trust for IP Awareness.

suit, and of course devices can be purchased elsewhere than on market-places, including via social media sites like Facebook.

The Industry Trust study also identifies a number of safety and security concerns associated with IPTV piracy:

(i) A number of Kodi add-ons require users to "pair" another device with their streaming box in order to allow adverts to be delivered to the device. This then exposes the device to what an array of malicious advertising including malware and other potentially unwanted programs, which can in turn lead to harm to user devices and theft of personal information; and

(ii) Younger users are exposed to inappropriate content through the add-ons themselves. The research carried out found that the customer interfaces of the most popular 16 add-ons provided no BBFC age ratings or indication of content suitability. In addition to content itself, users are exposed to inappropriate pop-up advertising of an adult nature. 1 in 10 users of unofficial apps and add-ons via IPTV boxes and sticks reported seeing offensive pop-ups or adverts.

Absent legislative intervention, the perceived legitimacy and cultural acceptability of accessing unauthorised content via illicit streaming devices will increase, and younger viewers will continue to be exposed to inappropriate content direct to the main family television set.

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.

Whilst there are limited examples (highlighted by the IPO in this Call for Views) of where existing laws have been used to successfully prosecute supply of illegal streams, in Sky's view the number of such convictions secured under existing legislation demonstrates that it is insufficient to tackle the growing problem. In the majority of cases, save for the single example called out by the IPO in its Call for Views, prosecutions of such offences are not being pursued under the CDPA due to the lack of directly applicable provisions in that Act. Examples of cases where prosecutions have not been pursued are set out in our answer to question 3 below and the reason for the shortcomings in the existing regime are detailed in our answer to question 4 below.

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.

Over the past year, Sky's anti-piracy team has identified over 100 cases involving illicit streaming devices. However, it has been extremely difficult to pursue these through to successful prosecutions.

Our engagement with Trading Standards has typically ended in frustration with repeated examples of Trading Standards feeling unable to prosecute using existing legislation.

Where cases have been taken up by PIPCU, resourcing issues and work pressures on that unit have meant that cases have not proceeded as quickly as we would have hoped.

It is our strong belief that these difficulties could be significantly alleviated by the introduction of legislation which is fit for purpose in light of new technological developments.

The following cases exemplify the problem:

Case A[8]

Following an investigation into an operation where live sports events were being streamed and made available on IPTV boxes via several websites, a referral was made to PIPCU in September 2014. Search and seizures were made in July 2015, and whilst the pirate was remanded in custody, he was later released. Two years later, the pirate has re-opened his site with the same name but moved from .net to .biz whilst the Crown Prosecution Service is still considering prosecution but without any meaningful action have been taken.

Case B

The defendant was selling set-top boxes which allowed users to watch all 380 Premier League games, Sky television channels without a legitimate subscription, and films which had not been officially licensed by the rights holders. Details were passed to Gateshead Trading Standards in January 2016. Following test purchases of the defendant's adapted Amazon Fire TV box, in March 2016, as part of Operation Kilimanjaro (a joint operation between FACT, the IPO, Northumbria Police, North East Scambusters and Trading Standards) IPTV boxes were seized from the homes of three suspects who were also arrested.

Solicitors established that the defendant had not committed any offences under Section 296ZB, Copyright, Designs and Patents Act 1988. The devices supplied did not enable or facilitate the circumvention of effective

[8] The names of the defendants and their URLs have been anonymized but Sky would consider disclosing such information to the Intellectual Property Office, on a confidential basis, on request.

technological measures i.e. that the technological measures (e.g. encryption) had already been circumvented by the original source of the illegal stream.

It was alleged that the defendant had committed offences under Section 7, The Fraud Act 2006 for making and supplying articles for use in frauds and under Section 44, The Serious Crime Act 2007 for encouraging or assisting offences i.e. by supplying devices preloaded with applications which gave direct access to illegal content and by posting updates and links on social media to illegal content.

However the Gateshead Council Litigation Team stated it was "unwilling to support the alleging of these offences". Gateshead Trading Standards stated that it would instead issue Written Warnings to the suspects. This concern about prosecuting other than under the CDPA exemplifies the approach of Trading Standard bodies nationwide.

Case C

In the context of a supplier of IPTV devices trading through a website, whose activities a Trading Standards body was investigating, Trading Standards expressed, in written correspondence, their unwillingness to take on a case involving the need to "fit" non-bespoke offences, such as those under the Fraud Act, to the activities carried out by IPTV suppliers, and highlighted their unease with the complexity of the existing laws.

In correspondence over a nine month period, the Trading Standards body was unwilling to alter their view despite Sky sharing legal advice and offering support, and eventually ignored all requests from Sky for updates. So far as we are aware, the case has been dropped and the site continues to trade.

In addition to these cases, we have made numerous referrals to law enforcement agencies but concerns over the lack of directly applicable offences have contributed to a reluctance on the part of law enforcement bodies to prosecute them.[9]

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.

In its Call for Views, the IPO sets out a number of provisions which "*may be applicable to the supply or use of set-top boxes for illegal streaming*". These range from copyright offences under the CDPA, to more general offences such as 'aiding and abetting' under the Fraud Act 2006, or 'encouraging offences' under the Serious Crime Act

[9] The names of the defendants have been anonymized but Sky would consider disclosing such information to the Intellectual Property Office, on a confidential basis, on request.

2007. The IPO also provides examples of where these provisions have been used to prosecute cases relating to the sale or use of illicit IPTV streaming devices or the provision of unauthorised content streams.

Sky considers that none of the provisions identified by the IPO provide adequate grounds for investigating or prosecuting the supply and use of devices through which unauthorised streams can be viewed, for the reasons set out below. This means that trading standards/enforcement agencies are often unwilling to investigate or prosecute the supply of illicit streaming devices.

Offences under the CDPA

S107 – Communicating a copyright work

In order to establish this offence it is necessary to prove that the accused communicated a copyright work to the public, either in the course of a business, or in a manner which "affects prejudicially" the owner of copyright, knowing or having reason to believe that he is infringing copyright in that work. The difficulty with relying on this offence in the context of suppliers of devices is that in many if not most cases there will be no communication of a work by the supplier of a device to end users. This may be true even in the case of a preconfigured or "fully loaded" device, because the seller is not directly communicating a specific work or works, but merely selling devices which can access them. It is certainly true in the case of a device which requires further configuration in order unlawfully to access infringing material.

s296ZB - devices and services designed to circumvent technological measures

Section 296ZB makes it an offence punishable on indictment with two years' imprisonment to advertise or deal in devices, products or components which are 'primarily designed, or adapted for the purpose of enabling or facilitating the circumvention of effective technological measures.'

In order to prove an offence under section 296ZB, it would be necessary to establish, *inter alia*, that the device in question had been either designed or adapted to enable or facilitate the circumvention of effective technological measures. The wording of this offence is tailored to devices which play some active part in bypassing the conditional access technology used to protect subscription television systems.

The issue with attempting to use this offence in prosecuting the supplier of a streaming device, such as a MAG 250 set-top-box, is that such equipment plays absolutely no part in circumventing any technological measures. The only role this type of equipment plays is to check the credentials of the user (in other words whether they are entitled to access the streaming server providing the content), and to convert the streamed content into pictures on the television screen. They are not designed to circumvent any technological measures because this circumvention has already taken place before the content is uploaded to the streaming server.

In such a pirate IPTV system, the encrypted transmission has usually been accessed through the purchase of a single valid subscription/viewing card which is used to decrypt the transmission. The decrypted transmission, instead of being used in the normal way by a genuine customer, is copied and digitised via an encoder and then uploaded to a server from which it is streamed to any number of illicit customers of the system. It follows that devices such as the MAG 250 do not circumvent any technological measure.

A further issue with relying on s296ZB is that the offence carries a relatively low maximum sentence of 2 years' imprisonment. The IPTV cases commonly considered for prosecution concern the supply of equipment to hundreds, if not thousands of customers, with six figure revenues accruing to the accused. Investigations into these offences are often protracted and complex, and it is simply not proportionate for the prosecutor to then be compelled to rely on an offence for which it is highly unlikely a first-time offender would face a custodial sentence particularly when the underlying wrongs, namely the copying of a copyright work carry a maximum sentence of 10 years' imprisonment.

S297 – fraudulent receipt of programmes

This is an offence which is aimed at consumers, not suppliers of devices. The only conceivable way it could be deployed against a supplier would be in the context of an inchoate offence of facilitating the s.297 offence. Proof of the requisite intent would be nigh-on impossible to establish, since it would first require establishment, to the criminal standard, of the dishonest intent of the end user, and then would require proof, also to the criminal standard, of the supplier's knowledge of the end user's criminal intent. It is not a viable basis for charging suppliers of devices.

s297A - unauthorised decoders

Section 297A criminalises the trade in 'unauthorised decoders', which are defined in this section as including 'any apparatus which is designed or adapted to enable (whether on its own or with any other apparatus) an encrypted transmission to be decoded'. An offence under section 297A carries a maximum penalty of 10 years' imprisonment on indictment. Exactly the same issues arise with respect to 297A as with 296ZB with reference to what function the equipment actually performs. The offence requires proof that the apparatus in question enables, either on its own or in tandem with other equipment, an encrypted transmission to be decrypted without payment of the appropriate fee. Again, the issue for the hypothetical prosecutor is how to prove that the device under consideration actually played any role in decrypting an encrypted transmission.

Sections 296ZB and 297A were designed for a version of television broadcast fraud which is increasingly being superseded by IPTV and which concerns the actual decryption of an encrypted signal, usually by means of the sharing of legitimate codes known as 'control words' between devices, a process colloquially referred to as 'card-sharing'. A well known such device is the Dreambox 500S set-top-box, which is able in effect to clone a legitimate smart card and create multiple clone set-top-boxes which share the control words of a legitimate card and use

such words, actively to decrypt the encrypted signal. Whilst 296ZB/297A are ideally suited to these 'card sharing' set-top-boxes, they were not designed for equipment which plays no part in decrypting content.

However, section 297A does represent, in Sky's view, the neatest legislative solution to the current lacuna. A series of relatively limited amendments, which focus on what the equipment or software deliver, rather than the means by which they deliver it, would (a) be in keeping with the original aim of the provision, (b) bring that section of the CDPA up to date and make it fit for use in relation to IPTV devices carrying unauthorised streams and (c) bring with it an element of future proofing, since the amended section would not be specific to a particular type of equipment/software or circumvention technique. The changes are set out below with amendments to the existing section underlined/struck through.

S297A Unauthorised ~~decoders~~ devices, &c

(1) A person commits an offence if he–

(a) makes, imports, distributes, sells or lets for hire or offers, or exposes for sale or hire any unauthorised ~~decoder~~ device;

(b) has in his possession for commercial purposes any unauthorised ~~decoder;~~device;

(c) installs, maintains or replaces for commercial purposes any unauthorised ~~decoder~~device; or

(d) advertises any unauthorised ~~decoder~~device for sale or hire or otherwise promotes any unauthorised ~~decoder~~device by means of commercial communications.

(2)A person guilty of an offence under subsection (1) is liable–

(a)on summary conviction, to imprisonment for a term not exceeding six months, or to a fine not exceeding the statutory maximum, or to both;

(b)on conviction on indictment, to imprisonment for a term not exceeding ten years, or to a fine, or to both.

(3)It is a defence to any prosecution for an offence under this section for the defendant to prove that he did not know, and had no reasonable ground for believing, that the ~~decoder~~device was an unauthorised ~~decoder.~~device.

(4)In this section—

"~~apparatus~~device" includes any ~~device~~equipment, component or electronic data (including software);

~~"conditional access technology" means any technical measure or arrangement whereby access to encrypted transmissions in an intelligible form is made conditional on prior individual authorisation;g~~

~~"decoder" means any apparatus which is designed or adapted to enable (whether on its own or with any other apparatus) an encrypted transmission to be decoded;~~

~~"encrypted" includes subjected to scrambling or the operation of cryptographic envelopes, electronic locks, passwords or any other analogous application;~~

"transmission" means–~~(a)~~ any programme included in a ~~broadcasting service~~ broadcast which attracts protections as a copyright work under Part 1 of the Act and in respect of which ~~is provided from a place in the United Kingdom or any other member State; or~~access is made conditional on prior authorisation,

~~(b) an information society service (within the meaning of Directive 98/34/EC of the European Parliament and of the Council of 22nd June 1998, as amended by Directive 98/48/EC of the European Parliament and of the Council of 20th July 1998) which is provided from a place in the United Kingdom or any other member State; and~~

"unauthorised" in relation to a ~~decoder~~device, means that the ~~decoder~~device is designed or adapted to enable ~~an encrypted~~a transmission, or any service of which it forms part, to be accessed in an intelligible form (whether on its own or with any other device) without payment of the fee (however imposed) which the person making the transmission, or on whose behalf it is made, charges for accessing the transmission or service~~(whether by the circumvention of any conditional access technology related to the transmission or service or by any other means).~~

Offences under the Fraud Act 2006

The Fraud Act 2006 contains offences under sections 6, 7 and 11 which, superficially, appear capable of adequately addressing IPTV crime, albeit they require proof of dishonesty on the part of the accused, an ingredient which is not required for offences under the CDPA.

Section 6, possessing articles for use in frauds, states:

Section 6

'A person is guilty of an offence if he has in his possession or under his control any article for use in the course of or in connection with any fraud.'

And section 7, making or supplying articles for use in fraud, states:

Section 7

(1) A person is guilty of an offence if he makes, adapts, supplies or offers to supply any article–

(a) knowing that it is designed or adapted for use in the course of or in connection with fraud, or

(b) intending it to be used to commit, or assist in the commission of, fraud.

Sections 6 and 7 appear on their face to be broadly drafted so as to capture a wide range of fraudulent conduct. In further support of the potential utility of these offences, since 'article' is defined within the Act as including 'any program or data held in electronic form', sections 6/7 appear to encapsulate both the hardware required for an IPTV network, and the apps/add-ons most usually associated with certain types of IPTV devices.

There is however a fundamental flaw in attempting to rely on sections 6/7 of the Fraud Act in an IPTV context since fraud is restrictively defined per section 1 of the Act:

Section 1

(1) A person is guilty of fraud if he is in breach of any of the sections listed in subsection (2) (which provide for different ways of committing the offence).

(2) The sections are–

(a) section 2 (fraud by false representation),

(b) section 3 (fraud by failing to disclose information), and

(c) section 4 (fraud by abuse of position)

In order therefore to make out the offences under sections 6/7, it is necessary to establish fraud by one of the three means defined above. Since neither fraud by failing to disclose information nor fraud by abuse of position can sensibly be made out even in theory in an IPTV context, the only route to establishing this form of statutory fraud sufficient to found an offence under sections 6/7 would be to prove a 'false representation'. Section 2 (fraud by false representation) provides that a person is guilty of such an offence if he,

Section 2

(a) dishonestly makes a false representation, and

(b) intends, by making the representation–

(i) to make a gain for himself or another, or

(ii) to cause loss to another or to expose another to a risk of loss.

(2) A representation is false if–

(a) it is untrue or misleading, and

(b) the person making it knows that it is, or might be, untrue or misleading.

(3) "Representation" means any representation as to fact or law, including a

representation as to the state of mind of–

(a) the person making the representation, or

(b) any other person.

(4) A representation may be express or implied

The issue arises as to what dishonest false representation is made by, for example, the supplier of a streaming device. Bearing in mind that the purchasers of such systems are often fully aware that they permit unlawful access to premium television content without payment (indeed that is why they are bought), there cannot be a false representation between seller and customer. Since a large proportion of these devices are sold only partially configured, it cannot be maintained that an implied false representation has been made by the seller of the device to the content owner or broadcaster, that the seller has a right to provide access to their content, since, at point of sale, many streaming devices are not so enabled. Any attempt therefore to use section 6/7 of the Fraud Act would lead to wholly unnecessary complexity, and at best a rather circuitous and artificial route to conviction via fraud by false representation.

Section 11 of the Fraud Act provides that a person is guilty of an offence if they obtain services dishonestly, and so again, appears at least in its wording to cater for systems such as IPTV networks which enable precisely such activity. However, IPTV devices are often offered for sale only partly configured, and therefore, in the state sold, not capable of accessing a service dishonestly (or at all). There is a lack of nexus between the seller of an IPTV device, the apps/add-ons which are often subsequently loaded onto the device to enable them to access content, and the providers of the illicit content themselves. Where therefore it might be possible to engage section 11 in certain scenarios, for example in circumstances where the supplier of a device also supplies the stream, it would not capture the more commonly observed criminality of the sale/supply of partly configured devices, without recourse to the additional complexity of alleging that the seller facilitated/encouraged the dishonest obtaining of services under sections 44-46 of the Serious Crime Act 2007.

Conspiracy to defraud (the position in Common Law)

There is currently only one offence which can adequately and effectively be used to prosecute IPTV fraud, and that is a common law conspiracy to defraud. This common law offence, unlike the Fraud Act, does not define 'fraud' restrictively, with the consequence that this offence is both available and relatively straightforward to deploy in an IPTV context.

The Common Law offence of 'conspiracy to defraud' was defined by the House of Lords in *Scott v Metropolitan Police Commissioner [1975] A.C. 819.* This judgment provided that it is an offence for two or more persons to agree to embark upon a course of conduct which they know or believe will defraud another or others. A person is defrauded when he is by dishonesty deprived of something which is his or of something to which he is or would or might be entitled or such interests are by dishonesty put at risk.

The ingredients of the offence may be summarised as follows:

(i) the accused dishonestly agreed with at least one other to embark upon a course of conduct,

(ii) at the time the agreement was formed the accused intended to act in accordance with the agreement.

(iii) The course of conduct which the conspirators agreed and intended to embark upon deprived the pleaded victims of something which was theirs or of something to which they would or might be entitled to but for the fraud or such interests were put at risk, and

(iv) the accused knew or believed that he had no right to deprive the pleaded victims or put their interests at risk.

In order to establish this common law fraud all that is required is that the defendant(s) 'deprived the pleaded victims of something which was theirs or of something to which they would or might be entitled to but for the fraud or such interests were put at risk'. This definition is far broader and capable of capturing a far wider spectrum of activity than the Fraud Act since its focus is on the effect, intended effect or potential effect of the actions of the accused.

The principal issues with reference to relying on common law conspiracy to defraud are as follows:

(i) In order to prove the offence you must prove the existence of an agreement between two or more people, and so the offence simply does not apply to lone traders (or to an agreement solely between a husband and wife);

(ii) The offence is triable only on indictment and its deployment against minor offenders might properly be regarded as excessive;

(iii) It is an offence the use of which has been discouraged by the Attorney General in Guidelines issued in January 2007 following the bringing into force of the Fraud Act 2006[10], albeit with the specific proviso within the Guidelines that it remains of particular utility for prosecutions concerning the theft of intellectual property.

(iv) It is an offence which the Crown Prosecution Service are reluctant to deploy[11]

(v) It is an offence which many Trading Standards Services are unable to prosecute because invariably their delegated authority will be limited to the conduct of proceedings in respect of statutory offences;

(vi) It is a common law offence, rather than one created by statute and is a 'catch all' rather than specific to the criminality alleged

With reference to the use of the common law offence, it ought to be noted that on 1 December 2016 a jury at Nottingham Crown Court found Terrence O'Reilly, guilty of two counts of conspiracy to defraud following a 5 week trial in the first UK prosecution of an IPTV supplier. The allegations concerned the operation and maintenance of a multimillion pound, pan-European organised crime group which harvested and redistributed broadcasts from over 20 major networks.

Whilst it ought to be recognised that conspiracy to defraud is the most useful currently available offence for addressing an IPTV scenario, and is often the preferred offence for prosecutors tackling complex intellectual property frauds generally, it ought not to be the only offence capable of being relied upon, particularly since it cannot address the issue of a sole trader.

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

Not to Sky's knowledge – it is not the jurisprudence per se which causes the problem in this area, it is the lacuna in the legislative framework.

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.

Evidence gathering can be challenging in cases involving significant suppliers, because of the need for digital forensic capability and resource, and the stretched resources of in particular specialist IP law enforcement bodies.

---

10 https://www.gov.uk/guidance/use-of-the-common-law-offence-of-conspiracy-to-defraud--6

11 In the Attorney General's Guidance on the use of Conspiracy to Defraud, Crown Prosecutors are obliged to maintain a record of their decision to use conspiracy to defraud on every occasion that the offence is selected (see paragraph 9) https://www.gov.uk/guidance/use-of-the-common-law-offence-of-conspiracy-to-defraud--6

This is an issue which would ideally be addressed separately to this call for evidence, although in Sky's view the introduction of a more focussed and bespoke offence is likely to reduce the evidential demands placed on law enforcement bodies, because it will be designed to apply to the activity in question, rather than law enforcement bodies having to "fit" other offences to the activity, with the additional evidential burden that exercise brings.

International considerations

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

As mentioned above, Sky provides pay-tv services in five EU member states. We have highlighted the inadequacies of the law to deal with illicit IPTV streaming devices with law enforcement authorities and government officials in all of our European markets, as well as the European Commission.

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

Sky notes that there is a significant international element to the supply chain of illicit IPTV boxes. As the IPO is aware, most of the boxes are manufactured in China and are frequently sold by Chinese vendors. Major online marketplaces such as Alibaba.com are an important part of the supply chain. A search for "fully loaded kodi" on 6 April 2017 yielded 13,081 results. A search on ebay.com for "fully loaded android TV" returned 1,488 listings, whilst the same search on ebay.co.uk returned 1,650 listings[12]

Enforcing intellectual property rights in an online environment is also very challenging because of the international element. Whilst we have made some progress by using the Notice and Takedown regime, recidivist hosting providers of servers and websites often locate themselves in other Member States and beyond, typically with less favourable enforcement regimes than the UK.

We also note that the content available through illicit IPTV devices is global in nature. This is particularly damaging for rights owners who sell premium content on a territorial basis. This poses real risks to the value that a broadcaster may wish to pay a rights owner for the exclusive licensing of that content in a territory.

[12] Searches performed at 3:55pm on 6 April

It would therefore be helpful if a specific offence of supplying devices intended for the purpose of infringing copyright was also introduced at the EU and international levels. In this respect, the UK should aim to act as a broker for increased cooperation with EU Member States and non-EU countries. For example, UK brokered Free Trade Agreements may be worth exploring as a means of ensuring a more consistent approach to the supply and support of illicit devices or streaming services, at the EU level (post-Brexit), and at the international level, in particular with key UK partners like China and Russia.

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. Other barriers to prosecution (resource, jurisdiction)

Efforts and legislation initiated by national governments vary from one country to another. Sky observes (and regrets) that a specific offence of supplying devices intended for the purpose of infringing copyright does not exist in any of the markets in which Sky operates. The IP enforcement regimes which do exist in those markets do not provide enforcement agencies with the powers (or the incentives) they require to adequately prosecute this form of activity. However, we are aware that certain jurisdictions do have more innovative approaches to enforcing IP in relation to these type of devices, for example the Canadian Courts have served injunctions prohibiting the sale of IPTV devices[13].

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

Yes, including law enforcement resource. However, in Sky's view the main barrier to the successful investigation and prosecution of these issues is the legislative gap we have highlighted above.

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?

Where criminal offences have been committed, Sky (and other rights holders) usually refer matters to law enforcement, often the PIPCU. However, PIPCU is a small unit with finite resource and the police more generally are stretched. It would be helpful if the powers which have been conferred to the police were extended to other enforcement agencies. For example, Trading Standards currently only have powers to investigate and prosecute under section 107 of the CDPA.

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? Other suggestions comments

---

13 See http://www.cbc.ca/news/business/android-box-free-tv-bell-rogers-1.4033741, and http://www.theglobeandmail.com/report-on-business/rob-commentary/canada-is-now-home-to-some-of-the-toughest-anti-piracy-rules-worldwide/article34223771/

In Sky's view, guidance would not help either the investigation or prosecution of the supply of IPTV devices. The issue at hand is whether existing laws empower enforcement agencies to successfully prosecute cases relating to the supply or use of illicit devices. Sky considers that they do not. That said, formal guidance from the IPO and from Trading Standards bodies clarifying that the supply of devices carrying unlawful streams, and the consumption of those streams by consumers, both constitute unauthorised and criminal activities would be helpful. There have been some distinctly unhelpful comments to the opposite effect by Trading Standards bodies in national press in recent months, which are irresponsible and short-sighted given the context that has led to the current Call for Views.

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

Sky understands that there will be no single answer to the problem. The challenge needs to be met on multiple levels including educational campaigns, use of technology, increased enforcement activity, and clearer laws which are simpler to enforce. However, the existence of a bespoke offence, which puts beyond doubt the criminality of the activities with which this Call for Views is concerned, would help content owners raise awareness of the issues with consumers and bring pressure to bear on third party intermediaries to support their enforcement and disruption efforts.

Information society providers (including market places, search engines, app stores and providers of social media services) have an important and growing role to play in combating the forms of illicit activity highlighted above. For example, links to live streams are widespread on social media platforms like Facebook or Twitter, and inexpensive streaming devices to which apps and software can be added are widely available to buy on online marketplaces. We continue to work with these providers, and note that Amazon has recently changed its listing criteria which has reduced the number of illicit devices offered for sale on their marketplace.

Finally, we believe that central, interconnected and appropriately resourced enforcement agencies should be set up at the EU and international levels, whereby the enforcement of the IP regime is seen as a priority.

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