Motion Picture Association – Written evidence (FDF0068)

Motion Picture Association (MPA) submission to the Lords Select Committee on the Fraud Act 2006 and Digital Fraud inquiry

The MPA welcomes the opportunity to respond to the call for evidence from the House of Lords Committee on the Fraud Act 2006 and Digital Fraud. We are grateful for the chance to share our views on what actions should be taken to tackle the increase in cases of fraud, and in particular fraud committed through digital services. We believe that MPA's extensive experience of tackling digital piracy, including successful UK prosecutions which often rely on the Fraud Act 2006, have given our forensic investigators an intimate knowledge of both how cybercriminals operate, what facilitates their activities, and most importantly what legislative measures may hinder their online operations, thus reducing harm to both businesses and consumers.

About the MPA

The MPA is the international trade association for the major companies that invest-in, produce, distribute and market film and television content in the UK: Walt Disney Studios Motion Pictures, Netflix Studios, LLC, Paramount Pictures Corporation, Sony Pictures Entertainment Inc., Universal City Studios LLC, and Warner Bros. Entertainment Inc. MPA member companies represent a key part of the UK film and television industry, both as significant inward investors and with a strong permanent presence in this country. The products and services of the film and television sector are important contributors to the success of the UK's high-growth, intellectual property-rich creative industries, which (even during the coronavirus pandemic) contributed £104bn in GVA and almost 2 million jobs to the UK economy in 2020[1].

Copyright (a type of intellectual property (IP) right) is the bedrock of the success of the UK's creative industries, as it allows creators of all forms of creative content, including audiovisual content, to exploit and generate revenues from that content, allowing a return on investments and subsequent investment in new content. The MPA works globally, in partnership with governments and law enforcement, to defend copyright against digital piracy and protect audiovisual creators and consumers from the economic and personal harms it causes, including through consumer education campaigns[2].

Overview

1. The primary focus of this submission is to show the importance of improving the transparency of online business interactions in the fight against digital crime; the links between digital piracy and digital fraud; and how solutions to improve transparency may therefore be beneficial to those engaged in the fight against both digital piracy and digital fraud.
2. We would also like to draw the Committee's attention to the growing phenomenon of "cybercrime as a service", which is driving proliferation of

[1] Oxford Economics report for the Creative Industries Federation, July 2021 (accessible here).

[2] See examples of UK education campaigns supported by MPA here, here and here.

both digital fraud and digital piracy, and thus increasing the urgency of adopting solutions focused on improving online transparency in business interactions.

3. In our view, an appropriate solution would be for the UK to implement and enforce an effective **"Know Your Business Customer"** (KYBC) obligation, requiring commercial entities to establish the true identity of their customers as a precondition of doing business. This would offer a tangible, complementary solution to existing laws regulating illegal and harmful activity online, whilst creating a minimal burden on legitimate businesses who are already in compliance. Improving the transparency of online business interactions in this way will be an effective tool in tackling both digital piracy and digital fraud

The problem

4. The MPA works globally on behalf of our members to advance policies that support creators, protect content and foster continued investment in a thriving creative economy. Unfortunately, **the proliferation of illegal and infringing content online (digital piracy) undermines the current UK policy framework and has a significant negative impact on jobs, growth and UK consumers**. This is because piracy not only impedes the evolution of legitimate channels for distribution of content but threatens to permanently damage or displace existing and authorised distribution channels, which are unable to compete with infringing business models.

5. Tackling digital piracy is crucial to delivering on the UK's ambitions to grow our IP-rich creative industries and to help protect consumers online. While there are a range of industry and law enforcement-led initiatives being deployed to achieve this aim – many of which are led or supported by MPA and its member companies – one of the greatest challenges remains the absence of reliable information on those commercial-scale pirates operating structurally-infringing services who are freely using legitimate business infrastructures, such as online hosting, advertising, payment processing and e-commerce platforms, to deliver illegal services.

6. The increasingly sophisticated and professionalised online piracy of TV, film and live sports content[3] is also a highly lucrative criminal activity that generates hundreds of millions of pounds every year for offenders. As a result, UK rightholders often rely upon various provisions of the Fraud Act 2006 to secure criminal IP convictions against the operators of illegal services.

7. The potential to rely on fraud offences was, for example, recognised in the UK Government consultation in 2018 regarding illicit set-top boxes, in which Government noted that section 11 of the Fraud Act 2006 ('obtaining services dishonestly'), coupled with section 44 of the Serious Crime Act 2007, were sufficient to "cover the criminality that arises in relation to illicit streaming devices" and provided the necessary sentencing powers for those offences. Examples of IP infringement cases in which fraud

[3] See The Royal United services Institute's 2021 "Taking the Profit Out of Intellectual Property Crime: Piracy and Organised Crime" report (accessible here).

offences have been relied upon include the *R v Rosero* case brought by Sky in 2016, and, more recently, in a number of prosecutions coordinated by the Federation Against Copyright Theft (FACT) relating to cases of illegal streaming of copyright protected material and the selling of illegal streaming devices[4].

8. The MPA's experience of dealing with online infringement in the UK, and that of other major UK rightholders, has shown that the growing complexity of investigating and tracing sources of illegal and infringing activity online is making the enforcement of IP rights increasingly difficult. Despite our extensive use of the tools already available under UK law to attempt to trace the operators of illegal services that trade in pirated content and counterfeit goods, experience shows **these efforts are increasingly thwarted by the ability of illegal operators to provide commercial services online under a cloak of anonymity, from anywhere in the world.**

9. Even where, after lengthy investigation, online intermediaries supporting illegal services are identified and contacted (for example, cloud, hosting and related infrastructure services), investigations often hit a dead end. This challenge has been recognised by Europol, which confirmed in its December 2020 *Internet Organised Crime Threat Assessment*[5], that "cybercriminals are […] proving to be highly aware of how to hide their identities and criminal activities from law enforcement or private sector companies."

10. In MPA's experience, the problem frequently comes down to the fact that the **online intermediaries providing the business infrastructure that enables the operation of the illicit service cannot supply any information that allows for the verification of the illegal service provider**. That, or the information they can provide has clearly been stolen, falsified, or is incomplete or otherwise misleading. The ease with which nefarious actors can remain anonymous in their underlying business transactions actively facilitates both digital piracy and potentially other crimes perpetrated online, including acts of digital fraud.

11. Furthermore, illicit businesses are proliferating in part due to the rise of the "cybercrime as a service" phenomenon, in which online vendors sell digital tools that make it easier to engage in cybercrime. Europol has identified Cybercrime-as-a-Service (CaaS)[6] as a cross-cutting crime facilitation challenge, noting, for example, its role in enabling phishing, malware, and ransomware. **MPA has seen the same CaaS phenomenon driving digital piracy as well, through the increasing prevalence of what we term 'piracy as a service'[7]** – a subset of the larger threat of CaaS. In the piracy context, this threat manifests itself as a suite of piracy facilitation services that make it very simple for any would-be pirate to create and monetise a fully functioning piracy operation. These services essentially lower the barriers to entry for the set-up and operation of commercial-scale piracy.

---

[4] See coverage of FACT's successful prosecutions here, here and here.

[5] See Europol's "Internet Organised Crime Threat Assessment 2020" (accessible here).

[6] Ibid

[7] A more detailed MPA briefing explaining 'Piracy-as-a-Service' is available on request.

12. Common examples are:
    - Ready-made website templates that facilitate the set-up of infringing streaming websites with a one-time payment
    - Content databases providing access to tens of thousands of infringing films and TV series
    - Internet Protocol TV dashboards and infrastructure
    - US Digital Millennium Copyright Act[8]-resistant Hosting Providers
    - Video hosting services that obscure links to infringing content
    - Third party software to quicken the process of uploading infringing content
    - Decentralised streaming software

13. PaaS is an emerging, and increasing sophisticated, piracy trend that needs to be better understood by policymakers and law enforcement in order to develop ways to address it and its negative impact on consumers and current and future investment in creative content.
14. Perhaps most pertinent to the Committee's inquiry is the fact that, in addition to the significant economic harm digital piracy causes to creators and creative businesses, **digital piracy, increasingly facilitated by PaaS, puts the individual consumers who access infringing content - knowingly or otherwise - at risk of fraud, malware and identity theft**.
15. A 2021 global study from online consumer safety group the Digital Citizens Alliance (DCA)[9], which used the advertising tracking technology of independent anti-piracy specialists White Bullet Solutions Limited to analyse piracy websites and apps, concluded that "while piracy causes direct harm to creators and others who lose income when their content is stolen, the impact goes well beyond the entertainment industry". This is because "**consumers who use piracy websites and apps are three times more likely to be exposed to malware**[10]."
16. Furthermore, whilst causing harm to both legitimate businesses and consumers, this investigation of content theft business models revealed that "the bad actors who operate in the illegal, underground market for pirated movies, TV shows, and other forms of content theft are reaping an estimated $1.34 billion in annual revenues through advertising on websites and illicit streaming apps."[11] When estimated revenues from advertising are combined with revenues from illicit subscriptions fees, the DCA estimates that the operators of piracy platforms generate "a combined $2.34 billion dollars in annual revenue."

---

[8] The US's Digital Millennium Copyright Act 1988 provides a 'notice and takedown' tool to help copyright holders get infringing user-uploaded content removed from websites.

[9] See Digital Citizens Alliance & White Bullet's August 2021 report "Breaking (B)ads: How Advertiser-Supported Piracy Helps Fuel A Booming Multi-Billion Dollar Illegal Market" (accessible here).

[10] In this context 'malware', in addition to 'malvertising', included 'Browser Hijackers', 'Keyword Loggers' for hacking usernames and passwords, and 'Trojan viruses' used to steal data.

[11] Ibid

17. This figure (which the report acknowledges likely undercounts the profits to be made from the digital piracy industry), combined with the emergence of PaaS (which removes the need for technical knowledge to establish an illegal service), makes the attraction of digital piracy to cyber-criminals all too clear.

The solution

18. MPA would like to see the UK Government taking the lead in addressing online piracy and the resulting risks to consumers by taking action to support rightholder and law-enforcement efforts to improve the transparency of online business interactions. The Royal United Services Institute's (RUSI) 2021 report 'Taking the profit out of intellectual property crime: piracy and organised crime' backed this need for action, underlining that: **"new 'know your business customer' (KYBC) rules are needed to ensure [online service] providers record and verify the identity of their business customers, denying service to rogue actors and providing law enforcement with crucial information when abuse occurs."**[12]

19. We believe this can be achieved through the simple introduction and enforcement of a **Know Your Business Customer (KYBC)** obligation on business infrastructure service providers that requires their commercial business customers to reveal their basic identity information - the kind of information that one would expect any legitimate business selling products or services on the high street to provide. Inspired by European and UK anti-money laundering regulations, a KYBC obligation would require commercial entities to establish the true identity of their business customers as a precondition for selling, and receiving payment for, digital services.

20. The means to achieve this are already provided for in UK Law under the Electronic Commerce Regulations 2002[13], but amendment is required to stop bad actors from simply choosing not to comply. Commercial entities that intentionally distribute illegal and harmful content online - be they scam website operators seeking to defraud, or services illegally distributing gambling, pornography, or other illegal content - can currently choose to ignore it and face no consequences for their failure to comply. A simple change in legislation to ensure that the current Electronic Commerce Regulations 2002's Regulation 6 is enforced would result in a real, tangible and complementary solution to tackling piracy, whilst at the same time creating a safer online environment for consumers, with minimal burdens on legitimate businesses.

21. Indeed, more stringent 'Know Your Customer' obligations are already in place in the field of financial services and compliance with the proposed KYBC obligation would be simplified courtesy of existing registers created in the context of the 5th Anti-Money Laundering Directive (2018/843/EU) of 30 May 2018. This Directive was transposed into UK law prior to the

[12] See RUSI's March 2021 "Taking the profit out of intellectual property crime: piracy and organised crime'' report (accessible here).

[13] See Regulation 6 "General information to be provided by a person providing an information society service" (accessible here).

UK's exit from the EU[14]. As a result, much of the information required for legitimate businesses to comply with a new KYBC obligation is already publicly accessible through national company registers[15], the European Business Register and the Ultimate Beneficial Owners register, all of which act as an important tool for businesses wishing to manage their own fraud risk.

22. A broad coalition of businesses and organisations in the UK and Europe (see Annexes 1 & 2) has been urging policy makers to develop, and effectively implement, a targeted KYBC obligation designed to prevent commercial entities with nefarious intent from continuing to act with impunity online and reduce harm to individuals and businesses. The breadth of this coalition highlights the fact that the accepted benefits of introducing a new KYBC obligation go well beyond MPA efforts to combat digital piracy.

23. Noting that the types of polycriminality than benefit from anonymity online are often integral to both digital piracy and digital fraud, we believe that KYBC, or a similar type of solution, could also help to reduce the prevalence of acts of fraud perpetrated online and their resulting harms to businesses and individuals. The fact that CaaS is driving the proliferation of threat actors across a wide spectrum of illegal activities means that, in our opinion, the need for KYBC obligations is growing increasingly urgent.

Potential barriers

24. One of the main barriers to swift and effective implementation of a KYBC obligation in the UK and EU is, ironically, the cross-cutting nature and types of harms (personal, social and economic) that anonymity in online business transactions can facilitate, as well as the wide range of types of legitimate business it ultimately harms: from film, music, sports and publishing to online sales of pharmaceuticals, children's toys and electrical goods. This means that efforts to introduce KYBC-style obligations have a broad support base but cut across the remit of multiple government departments, law enforcement and, potentially, different industry regulators.

25. The recently published UK Intellectual Property Office (IPO) IP Counter-Infringement Strategy 2022-2027[16] acknowledges that "government policy on IP is cross cutting and impacts nearly every sector. As such there is often significant overlap with the work of other departments". The IPO has recognised this challenge and the fact that "industry have been working collaboratively to identify potential solutions [to online infringement], for example the introduction of Know Your Business

---

[14] The UK opted out of transposing the 6th Anti-Money Laundering Directive (due 13 December 2020) only because most of its requirements are already covered by existing UK law. Registers established in the UK prior to the end of the transition period will remain (Source: https://www.lawsociety.org.uk/en/topics/brexit/anti-money-laundering-after-brexit).

[15] We note in this regard the government's intention, as expressed in its Corporate Transparency and Register Reform White Paper, to reform the powers and role of Companies House "with the ambition of being the most innovative, open and trusted registry in the world" and in so doing "boost Companies House capacity to combat economic crime." We understand these reforms will be introduced in the upcoming Economic Crime Bill in the 2022-2023 parliamentary session.

[16] See https://www.gov.uk/government/publications/ip-counter-infringement-strategy-2022-to-2027/intellectual-property-counter-infringement-strategy-2022-to-2027

Customer (KYBC) checks". As a result, their Strategy recommends the establishment of a cross-departmental forum since, "due to the cross-cutting nature of these issues, any action on these potential solutions would need to be take[n] forward in collaboration with other government departments".

26. MPA would welcome the support of members of the Lords Fraud Act 2006 and Digital Fraud Committee in encouraging Government departments, notably BEIS, DCMS, the Home Office, HM Treasury and the Ministry of Justice, to engage actively in the UK IPO's proposed cross-departmental forum, once established, and to support the ever-growing coalition in support of targeted KYBC obligations.

Conclusion

27. In setting out the importance of improving the transparency of online business interactions in tackling both digital piracy and digital fraud, we hope the Committee will recommend to Government the further development of KYBC-style solutions. These would help to reduce the harms to businesses and consumers actively facilitated by the ease with which bad actors can conduct their illicit online business in complete anonymity. We hope that drawing the Committee's attention to the growing phenomenon of "cybercrime as a service", which is driving proliferation of both digital fraud and digital piracy, has explained why such solutions are now urgently needed.

28. The UK has an opportunity to lead the way in implementing and enforcing an effective **"Know Your Business Customer"** (KYBC) obligation that requires commercial entities to establish the true identity of their customers as a precondition of doing business. This would offer a tangible, complementary solution to existing laws regulating illegal and harmful content and will reduce a wide range of online harms, whilst creating a minimal burden on legitimate businesses who are already in compliance. We, and KYBC's many supporters, ask simply that bad actors face consequences for their failure to comply with existing regulations, thus deterring them from repeat infringement.

ANNEX 1

Existing support for the introduction of targeted KYBC obligations

- ✓ **Europol**'s Internet Organised Crime Threat Assessment 2020 identified that *"with the growth of cloud services, a new modus operandi has emerged in which threat actors rent virtual private servers from legitimate hosting providers using fake or stolen identities. This highlights the need for stronger KYC [Know your customer] policies with businesses and organisations across the sector."*
- ✓ **The Royal United Services Institute (RUSI)** 2021 report Taking the profit out of intellectual property crime: piracy and organised crime underlined that: *"new 'know your business customer' (KYBC) rules are needed to ensure [online service] providers record and verify the identity of their business customers, denying service to rogue actors and providing law enforcement with crucial information when abuse occurs."*
- ✓ **The All-Party Parliamentary Group on Intellectual Property** made implementation of KYBC protocols one of the key recommendations of its Intellectual Property (IP) Enforcement 2021 report as a means to *"significantly enhance the UK's intellectual property enforcement regime and ensure creators, and businesses of all sizes, can continue to contribute to the cultural life of the UK and the economy*".
- ✓ **The Creative Industries Council** IP Subgroup - representing book and magazine publishers, major brands, the design community, fashion, film and TV, images, music, sports and video games - tabled a briefing paper in 2021 (see Annex 2) calling on "*policy makers urgently to consider the request to develop, and effectively implement, targeted KYBC obligations designed to prevent commercial entities with nefarious intent from continuing to act with impunity online*".
- ✓ **The KYBC.EU coalition** - 86 trade associations (see here) representing European and UK creative, children's toy, advertising, food and drink, online pharmaceutical, sporting goods and lighting industries companies, amongst others – called on EU legislators in an open letter in February 2022 to protect European consumers and businesses from online harms by ensuring that *"Know Your Business Customer obligations must apply to all intermediary service providers to offer a meaningful tool for tackling illegal activities and products online"* in the Digital Services Act. Unfortunately, EU co-legislators could only reach agreement on a KYBC provision with a scope narrowly limited to online marketplaces. The UK's exit from the EU thus

Annex 2 – Creative Industries Council KYBC Briefing Paper (September 2021)

"Know Your Business Customer" obligations

A briefing paper for UK policy makers from Rightsholders on the Creative Industries Council

Summary[17]

The growing complexity of investigating and tracing sources of illegal and infringing activity online is making the enforcement of IP rights increasingly difficult.

One solution is to enforce "Know your business customer" (KYBC) obligations, which require commercial entities to establish the true identity of their customers as a precondition of doing business. Such obligations offer a tangible, complementary solution to existing laws regulating illegal and harmful content and will reduce a wide range of online harms, whilst creating a minimal burden on legitimate businesses.

An obligation on service providers to make their own identification details accessible already exists under current UK and EU law (the 2001 E-Commerce Directive) but it is not enforced. Commercial entities that intentionally distribute illegal and harmful content online - be they scam website operators seeking to defraud or services illegally distributing gambling, pornography or other illegal content - simply choose to ignore it. They currently face no consequences for their failure to comply.

The rightsholder organisations on the Creative Industries Council IP sub-group that are listed in Annex 1 ask policy makers urgently to consider the request to develop, and effectively implement, targeted KYBC obligations designed to prevent commercial entities with nefarious intent from continuing to act with impunity online.

Such obligations will not only reduce harms to individuals, but also the significant economic harm to the UK's high-growth IP-rich Creative Industries, which - even during the coronavirus pandemic - contributed £104bn in GVA and almost 2 million jobs to the UK economy in 2020.

[17] For GVA and employment data please see: Oxford Economics report for the Creative Industries Federation, July 2021: https://www.creativeindustriesfederation.com/news/press-release-we-must-invest-creativity-new-data-reveals-creative-industries-are-catalyst-post

1. **What problem would the introduction of a KYBC obligation address?**

Many larger rightsholders in the UK have extensive experience using the tools available under UK law to attempt to trace the operators of illegal services that trade in pirated content and counterfeit goods.

But these efforts are increasingly thwarted by the ability of illegal operators to provide commercial services online under a cloak of anonymity, from anywhere in the world. Even where, after lengthy investigation, intermediaries supporting illegal services are identified and contacted (e.g. cloud, hosting and related infrastructure services), investigations often hit a dead end. The reason is that the intermediaries cannot supply any information that allows for the verification of the illegal service provider. Or the information they can provide is clearly false.

In too many cases, UK-based and overseas intermediaries who sell illegal operators the tools to operate their illegal businesses online simply don't know the identity or whereabouts of their own business customers, and are not incentivised to find out.

Both sides are presented with no risk for non-compliance, while the public, including UK rightsholders and consumers, bear the cost of the resulting proliferation of illegal and harmful content online.

Unmasking the true identity of the operators of illegal and harmful online services would lead to a reduction of such content online and would greatly facilitate consumers' and business customers' efforts to seek redress in respect of it.

The absence of accurate data about the identity of business customers also inhibits the ability to implement meaningful repeat infringer policies. It allows malicious actors to take advantage of companies that would otherwise be enforcing more responsible methods of addressing infringing behaviour.

An obligation on operators of online services to disclose their identity actually already exists: Article 5 E-Commerce Directive (ECD) as transposed into UK law by the Electronic Commerce (EC Directive) Regulations 2002 (E-Commerce Regulations), establishes that service providers shall render easily, directly and permanently accessible to the recipients of the service and competent authorities identity information, including:

- the name of the service provider
- the geographic address at which the service provider is established and
- the details of the service provider, including their electronic mail address

The above information should allow the operators of harmful and illegal services to be located and contacted rapidly and communicated with in a direct and effective manner. The problem is that commercial entities that intentionally distribute illegal and harmful content obviously choose not to comply with this obligation.

Introducing a KYBC obligation on <u>intermediaries that provide internet services to others</u> would require those intermediaries to ascertain and verify the identity details of their commercial customers, irrespective of their location, before any business can be conducted between the two. This would result in a real, tangible and complementary solution to the problem of non-compliance and fulfil the intent of Article 5 ECD, whilst creating a safer online environment with minimal burdens on legitimate businesses.

As the UK has left the European Union, we believe that the UK Government now has a perfect opportunity to exercise its sovereignty and close this loophole, thereby improving upon retained EU law and, in doing so, actively to support the UK's Creative Industries which, prior to the pandemic, were growing at five times the rate of the economy as a whole[18] and across all UK nations and regions.

2. Why does this problem exist?

Rightsholders face two problems when trying to identify the operators of illegal websites: firstly, operators of illegal websites simply choose not to comply with the current obligation resulting from the UK E-Commerce Regulations, i.e. that all service providers should make their contact details available on their websites; secondly, that intermediaries fail to obtain reliable contact information from their business customers, which include the operators of illegal sites.

Under EU (Article 8 Intellectual Property Rights Enforcement Directive – IPRED) and UK law, courts can order intermediaries to reveal the identity and contact details of the infringer of IP rights. Unfortunately, the intermediary is often unaware of, and unwilling to establish, the identity of the business customers to which they provide services. Under existing law, they face no consequences for failing to obtain this information.

In a flagrant contradiction to this, certain intermediaries are knowingly passing on the personal details of rightsholders, using platforms' reporting services, to infringers leading to serious and harmful consequences for individuals following up on infringements[19].

This status quo enables operators of scam websites seeking to defraud consumers, as well as operators of online services illegally distributing gambling, pornography, and other illegal and harmful content, to freely serve UK consumers, using UK and EU-based infrastructure, with an impunity borne of complete anonymity.

To illustrate the extent and seriousness of the problem a number of case studies, reflecting a range of sectors across the Creative Industries, are provided at Annex 2.

---

[18] *Ibid*, p. 7. The Creative Industries (CIs) contributed £111.7bn to the UK economy in 2018, a 43.2% increase in real terms since 2010. Between 2017 and 2018, the CI GVA grew by 7.4% in real terms, which is more than five times the growth rate of the UK economy as a whole. In employment terms, the CIs employed 2.10 million people in 2019, an increase of 34.5% from 2011.

[19] Please see British Association of Picture Libraries & Agencies case study in Annex 2 - Industry Cases Studies: Images.

3. Which categories of intermediary should be covered by a KYBC obligation?

When considering the categories of intermediary to be covered by KYBC obligations, it is necessary to find the right balance, recognising that the operators of sites and services distributing scams or illegal content are using a wide range of intermediaries in order to operate.

Against this background, we propose that **KYBC obligations should be applicable to the full range of services that enable the possibility of operating an information society service covered by the E-Commerce Regulations.** These would include, for example:

- User interactive platforms (e.g. retail marketplaces, social media platforms, messaging providers)
- Services that facilitate content delivery (e.g. file hosting services, cyberlockers, providers of dedicated content streaming servers)
- Providers of business hosting and/or Content Delivery Networks (CDN), such as Cloudflare
- Providers of web support services (e.g. registrars and registries, DNS services, proxy services)
- Providers of business support systems (e.g. email services, DNS services, financial services, advertising services)

For the avoidance of doubt, privacy protection companies should not suffice/be considered to be an individual customer for KYBC, i.e. they should have their own KYBC obligations and not act as a shelter for malicious actors.

4. What would be the impact on legitimate businesses?

KYBC obligations impose minimal or no burdens on legitimate businesses, all of which are easily identifiable.

Making a defined set of intermediaries responsible for collecting data to confirm the identity of business entities with whom they are directly contracting and who need their services to perform their online business activities - and verifying that data - should be easy to implement as part of the sign-up process and subsequent periodic re-verifications.

In the event the intermediary fails to, or is unable to verify the identity of its commercial customer, it will have to stop providing the services to the respective customer, which would provide an important disincentive against illegal or harmful activity.

Legislating to implement KYBC obligations would represent a codification of practices already adopted by a small number of the most responsible online players[20]. Unfortunately, such practices are very widely ignored and there is a strong case for harmonisation.

---

[20] The Anti-Counterfeiting Group offers examples of KYBC best practice for intermediary operators as follows:

- Provide a statement of company policies, a guide of expected standards and the consequences of disregarding

5. Sanctions

It is important to underline that the KYBC obligations proposed do not affect the liability privileges in the E-Commerce Regulations but create new and direct obligations on certain categories of intermediaries. Dissuasive financial penalties should be introduced for non-compliance.

ANNEX 1 – RIGHTSHOLDER SIGNATORY ORGANISATIONS

This paper is submitted on behalf of the following rightsholder organisations on the IP subgroup of the Creative Industries Council:

ACID – Anti-Copying in Design

BASE – British Association of Screen Entertainment

BBC Studios

BFI – British Film Institute

BPI (British Phonographic Industry) Ltd

British Fashion Council

BSkyB

English Premier League

FACT UK

Featured Artist Coalition

IFPI

ITV

Motion Picture Association

PACT

Publishers Association

Warner Bros

Warner Media

UKIE

UK Music

---

these principles, including the right to waive any confidentiality agreements as a result of failure or neglect.

- Check a customer's legal presence and state of affairs (company registration records, including VAT number, registered office address and commercial credit standing)
- Check the current business line. Does this match the stated specified objectives outlined in memorandum and articles of association?
- Check for previous penalties, judgements etc.
- Check customer reviews.
- Check customers' production and delivery channels, including source of manufacture, use of forwarding, postal and delivery services and compare routes and passages against known risk paths.
- Monitor performance, trade procedures and practices.

ANNEX 2 - INDUSTRY CASE STUDIES

The following case studies evidence the harm caused by identity concealment in online business interactions across the UK's Creative Industries. As well as clearly demonstrating economic harm, some examples also show how serious personal harms flow from economic harms, such as online piracy. Both types of harm are actively facilitated by a lack of transparency in the current system that can be easily rectified.

BOOKS

Publishers Association: File-sharing Websites

(example: 'Shadow' Library Genesis)

The Publishers Association is a member organisation for UK publishing, representing companies of all sizes and specialisms. Its members produce digital and print books, research journals and educational resources across genres and subjects.

Library Genesis is one of the most notorious pirate site networks harming members of the Publishers Association. It is listed on the European Commission's Piracy and Counterfeiting Watch List, and the site - plus several Library Genesis-linked sites - have been subject to 97a siteblocking in the UK.

Library Genesis offers illegal copies of copyrighted books (trade and academic), scientific journal articles, magazines, and other printed materials, frequently in cooperation with Sci-Hub, another notorious pirate site listed on the European Commission's Piracy and Counterfeiting Watch List.

The Library Genesis network has existed since 2008, yet the operators remain unknown. This is despite publishers' extensive efforts to enforce their rights, including civil litigation resulting in permanent injunctions against the site and its service providers, subpoenas to service providers, and multiple UK and EU siteblocking actions.

Library Genesis remains active to this day. The lack of a KYBC requirement has impeded publishers' efforts to hold the operators responsible for the infringement or otherwise end the infringement. The civil litigation and site-blocking efforts have resulted in ever-changing domain names and hosting providers, with no end to the piracy in sight.

BRANDS

Anti-Counterfeiting Group: Online Marketplaces (example: WISH)

The Anti-Counterfeiting Group (ACG) is a not-for-profit trade association respected as one of the world's leading specialists in the fight against the growing global trade in counterfeit goods. ACG represents its UK and EU members on the global stage, who together make up over 3,000 of the world's most prestigious brands.

WISH is an online platform, owned by WOWCHER, that offers products to consumers at huge discounts. Most of the goods sold on WISH have been identified as "suspicious" due to its pricing structure and the location of sale.

Moreover, test purchases by numerous ACG brands have evidenced the availability of counterfeits on the platform. Trader details are anonymised and payment for goods proceed via WOWCHER, making it very difficult to track and trace the actual seller.

Example - One brand, distrustful of products advertised on WISH, initiated an investigation into the trader. No trader details were displayed apart from a UK designation. The purchase was made via PayPal and the receipt received only showed that the recipient of the transaction as WOWCHER. No trader details were shown. Interaction with the trader was also via the platform, who acted as the intermediary.

Result - A test purchase was received, but no return address nor invoice was attached. The product was confirmed as counterfeit and a costly engagement with WOWCHER was initiated in an attempt to ascertain the actual supplier of the counterfeit goods.

Similar activities are regularly carried out on online marketplaces such as Etsy, Amazon and eBay, all of which are popular with counterfeiters. The implementation of KYBC obligations would

- ensure that sellers of counterfeit, potentially dangerous goods can be traced and brought to justice
- create a significant disincentive for sellers of counterfeit goods by removing their cloak of anonymity
- remove the administrative and financial burden of engagement with intermediaries who should know who their business customers are.

IMAGES

BAPLA: Social Media (example: Instagram)

The British Association of Picture Libraries & Agencies (BAPLA) represents over 115 picture library and agency members, providing the main source of licensed images seen every day in print and digital media, who in turn represent some

[21] BAPLA Research into Online Copyright Infringement, November 2019 https://bapla.org.uk/bapla-releases-its-first-online-copyright-infringement-report/

120,000 professional photographers, videographers and illustrators, many of which are SMEs or sole traders.

A report on online infringement[21] published by BAPLA in November 2019 showed:

- Overall, 93% of its members experience copyright infringement online
- An average of 25% of licensing revenue each year is lost to online infringements of images
- On a scale of 1-5, with 5 being the most difficult, 44% found reporting infringement on social media sites highly difficult.

In addition to these figures BAPLA is all too aware of the personal harm that can flow from economic harms, such as copyright infringement. Recently the organisation was alerted to a particularly serious incident of personal harm by a contributing photographer.

The case that follows exemplifies the need for a requirement for commercial entities, such as social media platforms, to reveal anonymous users in cases of commercial exploitation of copyright works.

A photographer's professional images were found on Instagram and the photographer used the platform's notice and takedown reporting service to request the removal of the copyright infringing images, which had been uploaded by anonymous users without his permission.

As a result of Instagram providing the anonymous users with the photographer's personal information (name and business email address) - which under their process has to be provided to the platform in order to prove copyright authority - the photographer suffered multiple death threats, vile messaging via email and experienced the setting up of accounts intended to ruin his small business. His family and friends were also researched and trolled.

For the sake of security, the photographer has taken his own professional website down and is no longer trading. He contacted a range of authorities but has so far barely made an impact. The police have taken no action and the ICO's policy is to review the case after three months. He has also contacted MPs with a view to having the case referred to the Minister for IP.

All the while the infringement of his photographs continues on various social media platforms, including YouTube, despite the fact that he does not post his images on social media.

Five months on, the situation has reached a blank wall with the ICO, who say they are unable to assist in the matter, and his case has not been followed up with the severity required. His images continue to be exploited by infringers, including taking credit for commercial uses. Due to his experience, understandably the photographer is reluctant to report further copyright infringement cases via social media reporting systems.

Several social media platforms inform rightsholders, who report infringements, that the platforms pass on the rights owner's name, email address, and the nature of the report, to the person who posted the content.

There is no obligation in such cases for users to reveal their identities reciprocally, nor any liability placed on these types of online intermediary to address the issue. This is a situation which can, and must, change.

Getty Images UK: Online Marketplaces (example: eBay)

BAPLA member, Getty Images UK, demonstrated in its recent evidence to the EU's Digital Services Act consultation that it is common to find third party sellers on online marketplaces who repackage and sell their copyright protected content without authorisation.

For example, a search on eBay (US), conducted on 5 September 2020 for the word "istock" - a registered trademark owned by Getty Images - returned multiple listings for users selling "any stock image" for well under market prices, including listings by commercial sellers who Getty Images had previously reported to the marketplace. Although eBay acted to remove the reported listings, the same seller brazenly relists shortly thereafter and eBay takes no additional action to stop this behaviour.

The introduction of KYBC procedures by online intermediaries, including online marketplaces, would act as a significant deterrent to such repeat infringers.

FILM & TV

Motion Picture Association EMEA: File-sharing websites (example: Openload)

The Motion Picture Association (MPA) represents the interests of the film, television, and streaming industry around the world. Its members distribute some of the highest quality and most popular audiovisual content and represent a key part of the UK film and TV industry, both as significant inward investors and with a strong permanent presence, including owning major UK production companies and facilities.

The MPA has extensive experience using the tools available under UK and EU law to attempt to trace the operators of illegal services. A high-profile example is Openload, a notorious pirate service that was listed on the Commission's piracy and counterfeiting watch list. Openload also provided back-office services for scores of websites on the UK Police Intellectual Property Crime Unit's Infringing Website List.

After a multi-year, resource-intensive investigation by MPA, this service was revealed to be hosted in and operated from within the European Union (EU), with infrastructure from EU service providers. When the MPA obtained a court order directing the EU hosting provider to identify its customer for Openload and two other pirate services, we hit a dead end: the listed customer was a defunct Hong Kong shell entity. The hosting provider admitted, despite having collected more than €19M in hosting fees, that:

"*The data communicated by our client are purely declarative. [Host] therefore does not possess any element permitting verification of authenticity.*"

Thus, the promise of transparent online businesses in the UK E-Commerce Regulations and ECD fails in practice because:

1. illegal operators do not voluntarily say who they are;
2. the people who sell them the tools to operate their illegal businesses simply don't know who they are and are not incentivised to care; and,
3. both sides are presented with very little risk for non-compliance.

The introduction of KYBC obligations in the UK would address this failure by forcing UK-based intermediaries to know exactly who their business customers are. In MPA's experience, concerted action on transparency in the UK and EU would have the added effect of significantly degrading the quality of the infringing services that pirate operators based overseas can provide to UK consumers by forcing them to use lower quality infrastructure based outside of Europe.

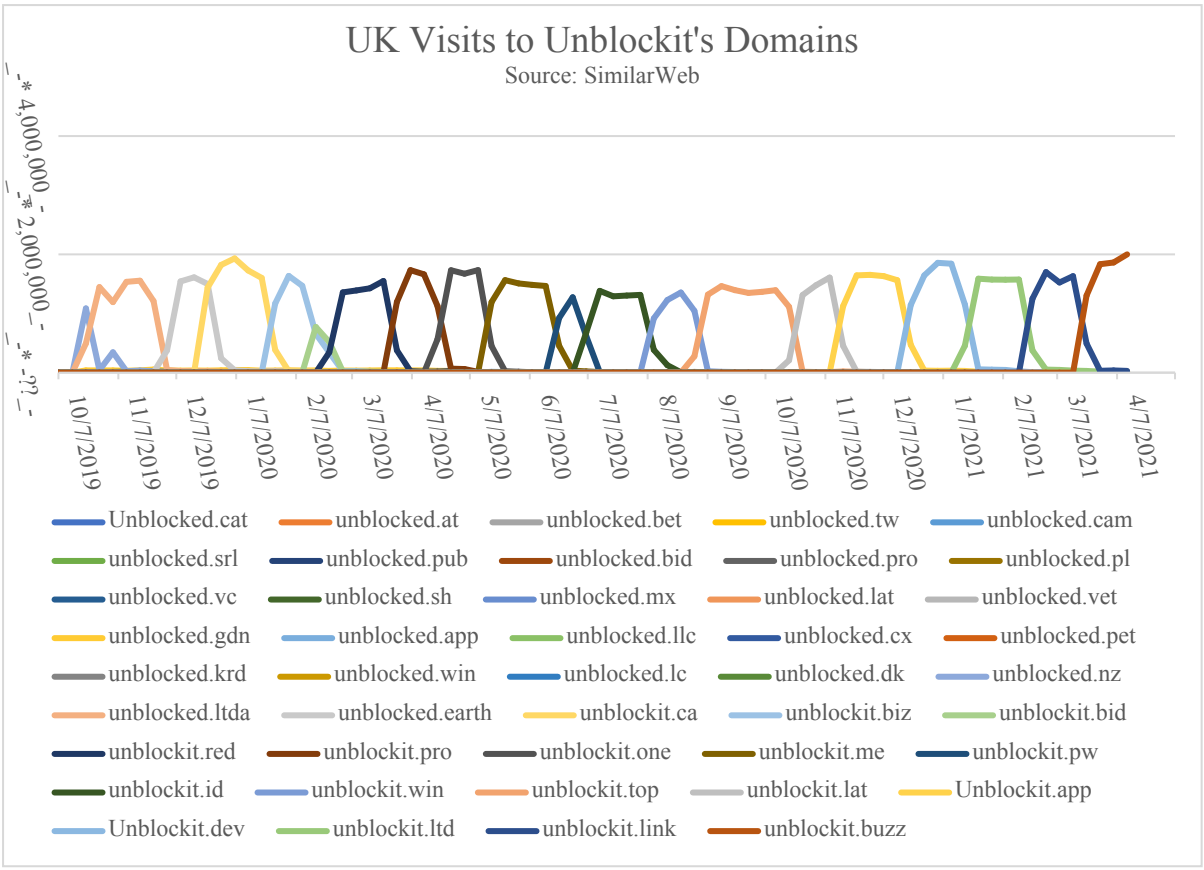
MUSIC

BPI: Proxy Servers (example: Unblockit & Cloudflare)

The BPI represents the UK's recorded music industry, championing the interests of small independent music labels alongside major record labels. As part of its work to protect the value of creative content and the livelihoods of UK music artists, BPI regularly comes up against websites such as Unblockit.

Unblockit is a Multi-Site Proxy Aggregator, acting as a signpost guiding ordinary users to websites that are blocked in multiple countries. In 2020, Unblockit was visited over 85 million times from the UK, in spite of the fact that many pirate brands it features are blocked under section 97 of the UK's Copyright, Designs and Patents Act.

Unblockit represents a particularly egregious example of 'domain hopping', i.e. the practice of relocating (hopping) to new domains to avoid being penalised. **In the absence of KYBC requirements, pirate site operators can register as many new domains as they like, in perpetuity.** When enforcement activities are implemented – be it ISP blocking, search engine delisting or otherwise – Unblockit and sites like it simply move to a new domain, as shown in the graph below.



To obscure its activities even further, Unblockit uses Cloudflare, a service that sits between the users and the server where the site is hosted.

Services like Cloudflare exacerbate the problem of domain hopping by masking the IP address of the hosting server, which complicates the investigation process. 75% of the sites currently being blocked at ISP level or de-indexed from search engines by BPI are registered with Cloudflare. Cloudflare has no KYBC procedures in place, which means that, even if they do suspend their services for a given domain, the site operator can immediately register a new one.

Unblockit is just one example of many sites which adopt the practice of domain hopping and rely on Cloudflare to circumvent and delay enforcement action. Indeed, domain hopping greatly benefits from the lack of enforcement of the current E-Commerce Regulations and has become an integral part of the business model of pirate sites. Government intervention is needed urgently to properly enforce the existing E-Commerce Regulations and ensure the effective delivery of industry-wide KYBC procedures.

BPI: Online marketplaces (example: eBay)

BPI also has extensive experience dealing with sellers of unlicensed music on eBay. In 2020, BPI removed 53,000 listings from online marketplaces, and 38,000 of these were from eBay.co.uk.

Sadly, it is a game of whack-a-mole, with a continuous repopulation of infringing listings by the same seller or different sellers, often suspected to be the same

individual(s). In fact, 13% of the listings removed from eBay in 2020 resurfaced under different listing IDs or seller accounts.

This repopulation was also observed while scanning the platform for unauthorised 2020 Record Store Day (RSD) releases, some of which reappeared on eBay *just 24 hours* after they had been removed. This event supports independent record stores, which have suffered terribly from the COVID-19 pandemic and subsequent lockdown measures, making this kind of flagrant infringement even more damaging in this context.

There is currently huge disparity in the way KYBC procedures are interpreted and implemented by different platforms. This can result in a concentration of infringement on platforms, such as eBay, where verification of sellers is insufficient, ineffective, or simply not taking place at all.

An effective KYBC verification system would ensure that offenders face real-world consequences and would deter them from re-listing infringing content under the same or different accounts.

SPORTS

Premier League: Internet Registries (example: Network Dedicated SAS & RIPE NCC)

The Premier League is the undertaking which organises and administers the Premier League football competition in England and Wales. The Premier League controls, amongst other things, the worldwide audio-visual rights to each Premier League match and is solely responsible for the licensing of the live audio-visual rights to all such matches in territories around the world. It works proactively and constructively with its Member Clubs and the other football authorities to improve the quality of football, both in England and across the world.

As part of an extensive global anti-piracy and IP protection programme, the Premier League frequently carries out detailed investigations to identify those responsible for providing unauthorised live streams of Premier League matches. This includes the organisations responsible for providing servers and Internet Protocol addresses that enable the delivery of illegal live streams of Premier League matches by pirate operators around the world.

An example of one such organisation is Network Dedicated SAS (AS62355), who receives its allocation of Internet Protocol addresses as a member of RIPE NCC, the regional internet registry serving Europe, Central Asia and the Middle East. The Premier League's investigations into Network Dedicated SAS show that the information provided about it on the RIPE NCC Database is not genuine. The physical address does not seemingly exist and the phone number provides no answer. The abuse email address has been provided with details of infringement over a significant period of time, but no response has ever been received and no action ever taken.

In the absence of enforcement of clear KYBC obligations, this registered RIPE NCC member has managed to avoid the consequences of its illegal activity over several years by simply hiding its true identity, despite extensive efforts by specialist investigators. Similarly, despite accepting Network Dedicated SAS as a member and allocating IP addresses to it, RIPE NCC has failed to obtain and maintain any accurate contact information for it.

10 May 2022