Whitehall Report 4-20

Taking the Profit Out of Intellectual Property Crime

Piracy and Organised Crime

Ardi Janjeva, Alexandria Reid and Anton Moiseienko

RUSI

Royal United Services Institute
for Defence and Security Studies

Taking the Profit Out of Intellectual Property Crime

Piracy and Organised Crime

Ardi Janjeva, Alexandria Reid and Anton Moiseienko

RUSI Whitehall Report 4-20, March 2021

Royal United Services Institute
for Defence and Security Studies

190 years of independent thinking on defence and security

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 190 years.

Published in 2021 by the Royal United Services Institute for Defence and Security Studies.

RUSI Whitehall Report 4-20, March 2021. ISSN 1750-9432.

Printed in the UK by Kall Kwik.

Cover image: Courtesy of Aliaksei/Adobe Stock.

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org

RUSI is a registered charity (No. 210639)

Contents

Acronyms

AV – audio-visual
CaaS – cybercrime as a service
CDD – customer due diligence
EUIPO – EU Intellectual Property Office
IAB – Interactive Advertising Bureau
IP – intellectual property
IPO – UK Intellectual Property Office (operating name of The Patent Office)
IPTV – Internet Protocol Television
ISD – illicit streaming device
IWL – Internet Watch List
KYBC – know your business customer
KYC – know your customer
MCC – merchant category code
MOU – Memorandum of Understanding
OCGs – organised crime groups
PaaS – piracy as a service
P2P – peer-to-peer
PUP – potentially unwanted programme
PIPCU – Police Intellectual Property Crime Unit
SAR – suspicious activity report
SOC – serious and organised crime
TAG – Trustworthy Accountability Group
VPN – virtual private network

Acknowledgements

The authors are grateful to the UK Intellectual Property Office, Alliance for Intellectual Property, Motion Picture Association, Industry Trust and the Premier League for co-funding this project. Their cross-sector cooperation reflects the spirit of the recommendations at the heart of this report.

Several organisations provided useful primary information for review by the authors. They include the funders, City of London's Police and Intellectual Property Crime Unit, BBC Studios, Asia Video Industry Association's Coalition Against Piracy, the World Intellectual Property Office and others who did not wish to be named.

The authors would also like to thank all interviewees, workshop participants and those who provided helpful feedback on earlier versions, namely Nick Court and Christian Chmiel. Last but not least, we are grateful to RUSI colleagues Dina Mansour-Ille, Demi Starks, Emma De Angelis, Zenab Hotelwala, Tom Keatinge, Keith Ditcham and Malcolm Chalmers for their support in reviewing and refining the report. The project's findings and recommendations were independently reached by the authors and were not influenced by the funders in any way.

Executive Summary

THE DISTRIBUTION OF copyright-infringing audio-visual (AV) content, also known as 'piracy', is a major profit-generating crime that offers significant opportunities for criminal gain. The idea that piracy is solely carried out by otherwise law-abiding, opportunistic individuals is no longer tenable. Piracy is an increasingly professionalised crime, yet the current response lacks the required urgency on numerous levels, from an incomplete understanding of pirate business models to the often low priority attached to tackling it by law enforcement agencies, regulators and online service providers and the limited awareness in the financial sector about intellectual property (IP) crime.

There is no standardised formula for estimating criminal income derived from piracy, but it is clear that significant proceeds move through the formal financial system each year. A 2019 EU Intellectual Property Office study suggests illegal Internet Protocol Television (IPTV) providers make nearly €1 billion a year supplying pirated content in the EU.[1] According to White Bullet – a cybersecurity and IP protection company – the 1,000 most popular pirate sites visited by UK consumers make up to £37 million a year from advertising in the UK alone; the top 10 of these are estimated to make £12 million. This rises to £460 million made by those same websites when including revenue streams from other countries.[2] Earlier studies arrive at even higher estimates.[3] The Trustworthy Accountability Group – a voluntary advertising industry initiative to combat criminal activity – estimates the top 672 pirate sites in the US alone generated $111 million in advertising revenue in 2016.[4]

This report explores how criminals make money from piracy and provides recommendations for how the UK government, law enforcement and private sector stakeholders can decrease the profitability of doing so. Its recommendations are addressed to UK audiences, but almost all of them are internationally applicable. This is particularly true of those aimed at rights holders, the financial sector and online service providers working across multiple geographies.

---

1. EU Intellectual Property Office (EUIPO), *Illegal IPTV in the European Union: Research on Online Business Models Infringing Intellectual Property Rights – Phase 3* (Alicante: EUIPO, 2019).
2. White Bullet Solutions Limited ('White Bullet'), <https://www.white-bullet.com/about-ipip>, accessed 19 February 2021. White Bullet provides research services to the EUIPO, mainly focused on advertising revenue from digital piracy.
3. Digital Citizens Alliance, 'Good Money Still Going Bad: Digital Thieves and the Hijacking of the Online Ad Business', May 2015, <https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/goodstillbad.pdf>, accessed 10 January 2021.
4. Ernst and Young, 'Measuring Digital Advertising Revenue to Infringing Sites', September 2017, <https://www.tagtoday.net/hubfs/Measuring%20digital%20advertising%20revenue%20to%20infringing%20sites.pdf?t=1507150221706>, accessed 10 January 2021.

The report begins by outlining current trends in AV piracy and mapping out the criminal actors involved, which range from individual offenders operating illegal streaming websites and cyberlockers[5] to transnational organised crime networks running illegal IPTV subscription services. Perpetrators at the sophisticated end of the spectrum operate transnationally, are able to maintain complex technical infrastructures and incorporate back-up systems to build in resilience in case of law enforcement action. The huge profits made by illegal IPTV operations are made possible by the rise of 'piracy as a service', a term used to describe how these groups sell software and expertise to new offenders to help them create their own operations selling IPTV accounts or illicit streaming devices. This report identifies four key revenue streams from piracy: advertising; direct payment; malware and fraud; and cryptomining. It explores the challenges and opportunities in frustrating criminals' attempts at monetising these activities, looking at ongoing and potential financial interventions in the UK and abroad.

It concludes that whole-of-system financial disruption efforts are needed to tackle piracy. Although the UK has made significant progress in championing a 'follow the money' approach to IP crime, more needs to be done. Every financial transaction in the piracy ecosystem represents an opportunity for disruption, yet very few financial institutions appear to understand their exposure to this crime type. While they are not indifferent to their regulatory obligations or the harm suffered by rights holders, there remains a distinct lack of awareness of how pirates monetise their operations. At present, the financial sector's engagement with piracy is overwhelmingly reactive and fails to draw on the wealth of open source intelligence available to inform client onboarding, develop typologies and refine transaction monitoring activities. This includes free and publicly available infringing website lists and information collected by rights holders and content protection agencies. These resources are integral to voluntary codes of best practice for advertising intermediaries, but virtually unheard of in the regulated financial sector.

Capitalising on existing intelligence requires a new public–private partnership with the purpose of information sharing across these actors, including rights holders, law enforcement agencies, financial institutions, online service providers (including internet service providers, domain name registrars, server hosting providers, social media and search operators) and advertising intermediaries. Greater information sharing ought to lead to a higher quantity and quality of suspicious activity reports filed by regulated entities, thereby producing often missing financial intelligence for law enforcement to draw upon in their investigations. In turn, law enforcement and government must ensure that parallel financial investigations are conducted as standard in suitable IP crime cases. This report finds this can only be achieved through a more coherent enforcement response which activates investigative skills and resources across the UK serious and organised crime policing network.

Beyond the financial sector, pirates' reliance on legitimate online service providers to run and monetise their operations gives rise to several vulnerabilities in their criminal business models.

5. Cyberlockers are third-party online data-hosting platforms that provide file-storing and file-sharing services for various types of media and data.

Currently, however, law enforcement and civil action is often undermined because these services do not verify their customers. New 'know your business customer' (KYBC) rules are needed to ensure these 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. Including these providers in a public–private partnership will enable them to be more proactive in vetting their customers.

At the same time, it remains true that much of the financial and online service provider infrastructure underpinning IP crime is located outside the UK's borders. Transnational cooperation is therefore essential. To date, there has been little effort to engage with financial regulators in key jurisdictions whose financial services are frequently misused by groups involved in piracy. Engaging with foreign regulators would send a strong signal by the UK that it views IP crime as a threat to its prosperity. The imposition of targeted financial sanctions on major criminal networks involved in IP crime could serve as such a signal and may be an important tool in tackling those operating from jurisdictions that are unlikely to cooperate with UK law enforcement agencies.

In total, the report makes 16 recommendations across the following five key areas of action:

1. **Reducing opportunities to monetise pirate operations** through the creation of a public–private partnership for intelligence sharing across government, law enforcement agencies, financial institutions, rights holders, online service providers and advertising networks.
2. **Preventing access to infringing websites and services** through continued engagement with online service providers, as well as a revision of their responsibilities in the context of KYBC practices.
3. **Disrupting payments for infringing content** through engagement with four key stakeholder categories:
    a. *Acquiring banks*, whose capacity to identify illicit activities by their customers should be reviewed by regulators in the UK and abroad.
    b. *Payment service providers*, who fulfil the same role as acquiring banks in some instances and should therefore be subject to the same regulatory scrutiny.
    c. *Card payment schemes*, who do not have transaction-level data and are therefore limited in their ability to identify criminal conduct but can take action based on intelligence supplied to them.
    d. *Crypto-asset service providers*, who account for a limited share of the piracy economy but may assume greater prominence in the future.
4. **Improving financial investigation and enforcement response to piracy**, including by creating a single intelligence system accessible to all UK agencies involved in policing IP crime that can be used to develop a better understanding of amounts of money made at various stages of the piracy supply chain.
5. **Reducing user demand for infringing content** by educating consumers on associated risks, such as fraud, malware infections, scams, high-risk advertising and malicious redirectors.

Introduction

GROWING FIVE TIMES faster than the UK economy as a whole, the UK's creative industries are an economic powerhouse that contributed an estimated 2 million jobs and £111.7 billion to the economy in 2018.[1] The film and TV industries contributed £20.8 billion to this figure in 2018 alone.[2] From the BBC to the Premier League,[3] the UK's cultural soft power draws on its thriving audio-visual (AV) entertainment sector.[4] Intellectual property (IP) rights including patents, trade secrets, copyright and trademarks are what enable creative businesses and individuals to achieve value from innovation, creation and production.

IP crime – defined here as the illegal manufacture, sale or distribution of trademark and patent protected goods ('counterfeiting') and/or copyrighted material ('piracy') – threatens this growth and economic prosperity. Counterfeit and pirated goods accounted for an estimated 3.3% of world trade in 2016, or 6.8% of all EU imports.[5] The OECD estimates that the infringement of UK companies' IP rights amounted to £11 billion in foregone global sales in

---

1. The creative industries were defined in the government's 2001 Creative Industries Mapping Document as 'those industries which have their origin in individual creativity, skill and talent and which have a potential for wealth and job creation through the generation and exploitation of intellectual property'. See Department for Digital, Culture, Media and Sport (DCMS), 'DCMS Sector Economic Estimates Methodology', <https://www.gov.uk/government/publications/dcms-sectors-economic-estimates-methodology/dcms-sector-economic-estimates-methodology>, accessed 3 February 2021; DCMS, 'DCMS Sectors Economic Estimates 2018: Employment', 26 June 2019, <https://www.gov.uk/government/statistics/dcms-sectors-economic-estimates-2018-employment>, accessed 14 November 2020; DCMS and Nigel Adams, 'UK's Creative Industries Contributes Almost £13 Million to the UK Economy Every Hour', press release, 6 February 2020, <https://www.gov.uk/government/news/uks-creative-industries-contributes-almost-13-million-to-the-uk-economy-every-hour>, accessed 10 November 2020.
2. DCMS and Adams, 'UK's Creative Industries Contributes Almost £13 Million to the UK Economy Every Hour'.
3. Across the BBC, services are reaching more people globally than ever before – in 2020 this was more than 468 million each week, an increase of 11% on 2019. See *BBC News*, 'BBC News Reaching Highest Ever Global Audience', 23 July 2020. Cumulative audiences for live Premier League programming rose 11% to 1.35 billion in 2019. The Premier League was shown in a total of 188 of the world's 193 countries recognised by the UN. See Premier League, 'Premier League Global Audience on the Rise', 16 July 2019, <https://www.premierleague.com/news/1280062>, accessed 3 February 2021.
4. Christopher Hill and Sarah Beadle, *The Art of Attraction: Soft Power and the UK's Role in the World* (London: British Academy, 2014).
5. OECD and EU Intellectual Property Office (EUIPO), *Trends in Trade in Counterfeit and Pirated Goods* (Paris: OECD Publishing, 2019), p. 3.

2016, or 2.1% of total sales that year.[6] IP infringement places a significant burden on rights holders and law enforcement, and deprives governments of billions in tax revenue each year.[7] Frontier Economics estimated global digital piracy was worth $213 billion a year in 2015.[8] In 2019, the US Chamber of Commerce estimated global film piracy costs their domestic economy $29.2 billion a year in lost revenue.[9]

In 2019, a joint Europol and EU Intellectual Property Office (EUIPO) study confirmed that IP crime is increasingly carried out by sophisticated organised crime networks, posing a growing national security threat across Europe.[10] This is supported by UK law enforcement data which shows domestic organised crime groups (OCGs) engaged in IP crime are commonly linked to benefit fraud, loan sharking and drug dealing.[11] Today, some criminals can make more money selling counterfeit goods than they can from trafficking controlled drugs.[12]

Yet, while the involvement of OCGs in counterfeiting is well evidenced,[13] there is less research on piracy as an organised crime type or its significant revenue opportunities. Although the term 'IP crime' is useful, there is little evidence to suggest piracy and counterfeiting is carried out by the same actors. Moreover, both trades differ in their means of monetisation and enablers (both legal and illegal).[14] This means the measures required to investigate and disrupt piracy are often distinct from those needed to combat counterfeiting. This report therefore looks at

6. OECD and UK Intellectual Property Office (IPO), 'Trade in Counterfeit Products and the UK Economy: 2019 Update', 2019, p. 5.
7. EUIPO, *2020 Status Report on IPR Infringement: Why IP Rights Are Important, and the Fight Against Counterfeiting and Piracy* (Alicante: EUIPO, 2020); Europol and EUIPO, 'Intellectual Property Crime: Threat Assessment 2019', 2019, <https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_IP_Crime_Threat_Assessment_Report/2019_IP_Crime_Threat_Assessment_Report.pdf>, accessed 7 November 2020.
8. Frontier Economics for the International Chamber of Commerce's Business Action to Stop Counterfeiting and Piracy (BASCAP), 'The Economic Impacts of Counterfeiting and Piracy', 2016, p. 7, <https://iccwbo.org/publication/economic-impacts-counterfeiting-piracy-report-prepared-bascap-inta/>, accessed 11 February 2021.
9. David Blackburn, Jeffrey A Eisenach and David Harrison Jr, 'Impacts of Digital Video Piracy on the U.S. Economy', NERA Economic Consulting, Global Innovation Policy Center and the US Chamber of Commerce, June 2019, <https://www.theglobalipcenter.com/wp-content/uploads/2019/06/Digital-Video-Piracy.pdf>, accessed 3 February 2021.
10. Europol and EUIPO, 'Intellectual Property Crime', p. 40.
11. IPO, 'IP Crime and Enforcement Report 2017/2018', 2018, p. 13.
12. OECD and EUIPO, *Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact* (Paris: OECD Publishing, 2016).
13. Europol and EUIPO, 'Intellectual Property Crime Threat Assessment 2019', 2019, p. 3; Europol and EUIPO, '2017 Situation Report on Counterfeiting and Piracy in the European Union', June 2017.
14. European Commission, 'Counterfeit and Piracy Watch List', Commission Staff Working Document, 14 December 2020, <https://trade.ec.europa.eu/doclib/docs/2020/december/tradoc_159183.pdf>, accessed 10 January 2021; Europol, 'Intellectual Property Crime', <https://www.europol.europa.

the strategies and tools that could facilitate the financial disruption of piracy as a standalone subject, focusing on the infringement of film, TV and live sports content.

Growing recognition of the scale and national security threat posed by OCGs involved in IP crime has generated interest in the application of 'follow the money' approaches, defined by the European Commission as 'policy measures that identify and disrupt the money trail for commercial scale IP right-infringing activities, diminishing their profit-making potential'.[15] Since 2011, the European Commission has championed two Memorandums of Understanding (MOUs) with private sector intermediaries whose services are commonly abused in order to facilitate IP crime. Signed in 2011, the first is devoted to bringing together online platforms, rights owners and industry associations to limit the offer of counterfeit goods on online marketplaces. The second, which was signed in 2018, is a voluntary agreement between advertising intermediaries, advertisers, technology providers and industry associations to prevent adverts being placed on websites hosting pirated content.[16]

The UK's current IP Enforcement Strategy (2016–20) also champions a 'follow the money' approach, advocating for greater use of financial investigations and the 2002 Proceeds of Crime Act in IP crime cases.[17] The UK's forthcoming IP enforcement strategy, to be released in 2021, will maintain this commitment to the greater use of financial investigations and asset recovery in IP crime cases, supporting relevant enforcement agencies across the UK to pursue this approach. There are at least six dedicated financial investigators and a further six financial intelligence officers working across the UK Intellectual Property Office (IPO) Intelligence Hub and the City of London Police Intellectual Property Crime Unit (PIPCU).

---

eu/crime-areas-and-trends/crime-areas/intellectual-property-crime>, accessed 3 February 2021; Europol and EUIPO, 'Intellectual Property Crime'.

15. European Commission, 'Enforcement of Intellectual Property Rights', <https://ec.europa.eu/growth/industry/policy/intellectual-property/enforcement_en>, accessed 3 February 2021. See also European Commission, 'Industry-Led Initiative to Fight Counterfeiting Gets New Boost', 2019, <https://ec.europa.eu/growth/content/industry-led-initiative-fight-counterfeiting-gets-new-boost_en>, accessed 3 February 2021; Europol and EUIPO, '2017 Situation Report on Counterfeiting and Piracy in the European Union', p. 54; IPO, 'IP Crime and Enforcement Report 2019 to 2020', September 2020, p. 106.
16. European Commission, 'Memorandum of Understanding on the Sale of Counterfeit Goods on the Internet', <https://ec.europa.eu/growth/industry/policy/intellectual-property/enforcement/memorandum-understanding-sale-counterfeit-goods-internet_en>, accessed 3 February 2021; European Commission, 'Memorandum of Understanding on Online Advertising and IPR', <https://ec.europa.eu/growth/industry/policy/intellectual-property/enforcement/memorandum-of-understanding-online-advertising-ipr_en>, accessed 3 February 2021 .
17. IPO, 'Protecting Creativity, Supporting Innovation: IP Enforcement 2020', 2016, pp. 21–22.

This report contributes to the 'follow the money' approach[18] to piracy by analysing how criminals make money by distributing pirate content online and providing recommendations on how UK government, law enforcement and private sector stakeholders can undermine the profitability of those criminal business models. In doing so, the report focuses on the following areas:

- **Exposing the continued reliance of criminal business models on the exploitation of legitimate business sectors, which provides opportunities for disruption**. This includes financial intermediaries, advertising intermediaries and online service providers such as internet service providers, domain name registrars, server hosting providers, social media and search operators, all of whom are in a position to either constrict criminals' ability to profit from piracy or help facilitate law enforcement action by sharing or acting on relevant intelligence.
- **Identifying how financial intelligence and investigations can help disrupt illicit financial flows derived from piracy**. Disrupting criminals' ability to make and receive payments through the formal financial sector is crucial in reducing criminal revenue streams.
- **Publicising the harm to individual consumers of pirated content**, which can facilitate reduction in consumer demand. These harms include viruses and malware transferred through piracy sites, sometimes culminating in identity theft and fraud. It does not cover how revenues from piracy may fund cyber attacks and other forms of serious organised criminality, which remains an intelligence gap.[19]

This report aims to contribute to existing literature on the demonetisation of piracy and therefore the reduction of incentives for criminals to be involved in this crime. The authors believe this to be the first research project on this topic to synthesise different perspectives across law enforcement and industry to produce recommendations for key stakeholders in the UK.

18. There is no standard definition of 'follow the money'. The European Commission's use of the term focuses on disrupting all opportunities for financial gain, whereas the UK's IPO IP Enforcement Strategy primarily refers to the identification, seizure and recovery of criminal gain from IP crime. This report follows the definition used by the European Commission, which the authors take to include asset identification, seizure and recovery activities. See IPO, 'Protecting Creativity, Supporting Innovation: IP Enforcement 2020'; European Commission, 'Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee: A Balanced IP Enforcement System Responding to Today's Societal Challenges', COM(2017) 707 final, 29 November 2017, <https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-707-F1-EN-MAIN-PART-1.PDF>, accessed 5 February 2021.
19. Notwithstanding Europol and EUIPO, *IP Crime and Its Link to Other Serious Crimes: Focus on Poly-Criminality* (Alicante: EUIPO, 2020).

Methodology

The report relies on the following methods for data collection and analysis as part of this research project:

- **A targeted literature review** of IP crime-related and piracy-specific reports by international organisations, governments, academic experts, court case materials and news reports.
- **Semi-structured research interviews with 77 experts** using an interview protocol that was adjusted as necessary depending on the interlocutor's area of expertise and the context of the conversation. These interviews were conducted between February and September 2020. The protocol was sent to interviewees in advance. In most cases, conversations covered IP crime-related criminal risks and responses to them in the country or field in question, including the role of the private sector and intermediaries. Experts interviewed included: UK and EU government officials; law enforcement; online service providers; financial sector compliance officers; rights holders; rights holders' industry associations; content protection providers; and academic experts. The majority of interviews were conducted using video-conferencing software due to the coronavirus pandemic. Interviewees were identified through the literature review, snowball sampling and a widely circulated press release inviting self-nominations. Wherever possible, interview findings are triangulated with open source references.
- **A review of primary data** including quantitative survey data, information from historic and ongoing private investigations, and qualitative data from victims of piracy-related fraud. This valuable data was provided to the researchers by the research funders, City of London Police Intellectual Property Unit (PIPCU) and other sources who wished to remain unattributed. Where this information is not publicly available, it is reproduced in this report. It is, however, not possible to reproduce or reference all the evidence submitted due to the sensitivity of the material. For ethical reasons, the authors have not provided direct links to pirated content or web resources that facilitate access to it.[20] Likewise, findings have been reviewed to minimise the risk of providing information valuable to the perpetrators of IP crime.

20. Lists of infringing sites include the European Commission's Counterfeit and Piracy Watch List, the World Intellectual Property Organization's WIPO Alert platform, the Office of the US Trade Representative (USTR)'s Annual Special 301 Report on Intellectual Property Protection and Review of Notorious Markets for Counterfeiting and Piracy, and City of London Police Intellectual Property Unit's (PIPCU) Internet Watch List (which is specific to the UK). These lists are regularly updated. See European Commission, 'Counterfeit and Piracy Watch List'; Office of the USTR, 'USTR Releases Annual Special 301 Report on Intellectual Property Protection and Review of Notorious Markets for Counterfeiting and Piracy', press release, 29 April 2020, <https://ustr.gov/about-us/policy-offices/press-office/press-releases/2020/april/ustr-releases-annual-special-301-report-intellectual-property-protection-and-review-notorious>, accessed 3 February 2021; iab.uk, 'The Infringing Website List (IWL)', 23 March 2016, <https://www.iabuk.com/policy/infringing-website-list-iwl>, accessed 3 February 2021.

- **Expert validation workshops**. Original drafts of this report were discussed in two one-hour online validation workshops in January 2021. Participants included representatives of the financial services sector and cross-sector IP crime experts from law enforcement and industry, excluding representatives of the funders. Revisions were made based on feedback the researchers received in these sessions.

Structure

The report begins by explaining the key criminal distribution methods for pirated content before turning to how illicit financial gain is derived from piracy and how this can be disrupted. Chapter I explores the involvement of organised crime networks in piracy, charting high-level trends in the consumption and distribution of pirated film, TV and live sports. It also provides an overview of the stakeholders involved in responding to piracy. Chapter II analyses how criminals make money from piracy, examining the advertising and subscription models that are the bedrock of piracy operations. Chapter III explores the challenges and opportunities in frustrating criminals' attempts at monetising this activity, looking at ongoing and potential financial interventions in the UK and abroad. The report concludes with policy recommendations for the public and private sector, including law enforcement, rights holders, advertising intermediaries and the financial sector.

I. Trends in Piracy and Organised Crime

THIS CHAPTER BEGINS by defining the terminology used to capture the most popular methods of distributing and consuming infringing content, before turning to high-level consumer trends in film, TV and live sports piracy in the UK (Table 1). It then details how pirate distribution models have become more sophisticated and professionalised over time, with piracy operations now perpetrated by a mixture of technically skilled and well-coordinated OCGs as well as individual offenders. It explores the extent to which pirates are engaged in multiple types of crime (poly-criminality), detailing their involvement in fraud, malware and identity theft. It then turns to the UK enforcement structure as it currently stands, reflecting on the challenges posed by the modern piracy ecosystem. This contextualises the subsequent chapters, which focus on the monetisation of piracy and interventions required to disrupt it.

Table 1: Key Terminology and Most Popular Online Methods of Piracy Consumption in the UK

Source	Explanation
Internet Protocol Television (IPTV) Piracy	
Through apps/services preloaded onto **illicit streaming devices, such as Kodi*** **boxes** (usually a one-off payment) A **paid subscription** to an illegal IPTV piracy provider that gives access to infringing content through an app or other internet-enabled platforms (usually a monthly or annual subscription payment)	IPTV is the technical term for the delivery of television content over the internet (in contrast to traditional terrestrial, satellite and cable formats). Legal examples of IPTV services include Netflix, Amazon Prime Video, Hulu and BBC iPlayer. Pirates exploit IPTV technology to provide illegal access to thousands of live TV channels and on-demand content through physical devices and apps/add-ons. This content is usually only otherwise available across multiple separate (paid) legitimate services, or not available legally in their country or region. **Physical Devices and Apps** Streaming devices and viewer hardware such as set-top boxes and Amazon Fire TV Sticks are legal when used to watch legitimate free-to-air or paid content. They become 'illicit streaming devices' (ISDs) once they are adapted to access or distribute copyright-infringing content.† Adapting a streaming device to view illicit content usually requires loading of apps, software add-ons or extensions. Illegal Kodi extensions are a well-known mechanism for doing this. ISDs can come as 'pre-loaded' set-top boxes that can be plugged into a TV (as one would with a DVD player) to access unlimited illegal content provided by pirates, without downloading specific features. This software can be uploaded by a single user or by a 'reseller' who buys a significant number of boxes with the intention of altering and selling them as ISDs on an ongoing basis. The abuse of otherwise legal set-top boxes makes enforcement challenging because each device can be easily altered using accessible information online, enabling relatively simple access to illegal content without a high degree of technological capability. Access to illegal IPTV can also be secured via a one-off payment or a monthly/annual subscription to an app or add-on that can be accessed through any internet-enabled device such as a smart TV or handheld device such as a laptop, tablet or smartphone. Piracy apps are usually downloaded from 'unofficial' app stores and websites, but in some instances are also available on mainstream app stores. Alternatively, users might be encouraged to download a generic app, such as a legal video player, and given instructions on how to access IPTV content. Illegal IPTV apps look slick and professional and often come with access to customer support and advice from the pirate operator.

Source	Explanation
Other	
BitTorrent or another file-sharing or **peer-to-peer (P2P) service**	BitTorrent is a P2P file-sharing protocol designed to reduce the bandwidth required to transfer files. It does this by distributing file transfers across multiple systems, thereby lessening the average bandwidth used by each computer. For example, if a user begins downloading a movie file, the BitTorrent system will locate multiple computers with the same file and begin downloading the file from several computers at once.[‡] This used to be the most popular method of infringing content.[§] Continually improving internet infrastructure has seen 'hosting websites' that directly stream or enable downloads of infringing content become a competing method of distribution.
A website which **hosts** or **links** to full-length infringing content	Hosting sites, also known as 'illicit streaming sites', enable the user to download infringing content or watch directly through embedded media players. Traffic is constantly driven to hosting sites by 'linking sites' that aggregate, categorise and organise indexes of URLs of where infringing content can be accessed.[‖] In 2016, the European Court of Justice ruled that linking to infringing content is illegal unless it is done 'without the pursuit of financial gain by a person who did not know or could not reasonably have known the illegal nature' of the content.[¶]
Cyberlockers	Cyberlockers are third-party online data-hosting services that provide file-storing and file-sharing services for various types of media and data. Although many cyberlockers are genuine file storage facilities, some knowingly host large volumes of pirated content. The European Commission notes that there is a 'clear difference' between legitimate and rogue cyberlockers, because the latter 'incentivise their users to upload popular [infringing] files to their servers' and register companies offshore to conceal the identity of their operators.[**]
Receiving through email, via a USB stick, through a site like Dropbox, or **links to film/TV downloads in a messaging app**	Messaging apps like Discord and Telegram are also used to distribute links to pirate content. Private Facebook groups are also a popular medium for sellers to offer '24-hour free codes' and acquire payment details for future sales.[††]

Source	Explanation
Live broadcasts or infringing copies of audio-visual content streamed, hosted or advertised on 'grey sites' like YouTube or social media sites such as Facebook, Telegram or Twitter (not by an official source)	Some social media platforms are used to advertise illegal IPTV services or provide customer support to IPTV users.
Stream ripping using software, an app, browser extension or online converter (free to download)	These allow consumers to download film/TV programmes/episodes from an online streaming website, converting it into a format which enables successful viewing from whatever device the consumer is using.

*Sources: * Kodi is legal software designed to play personally owned media and legally accessible content on the internet. However, the software can be altered with third-party add-ons to give access to pirated content; † IPO, 'Guidance: Illicit Streaming Devices', 20 November 2017, <https://www.gov.uk/government/publications/illicit-streaming-devices/illicit-streaming-devices#:~:text=Illicit%20streaming%20devices%20are%20physical,%2C%20free%20to%20air%2C%20content>, accessed 13 November 2020; ‡ See Tech Terms, 'BitTorrent', <https://techterms.com/definition/bittorrent>, accessed 3 February 2021; § MUSO, 'Global Piracy Increases Throughout 2017, MUSO Reveals', 21 March 2018, <https://www.muso.com/magazine/global-piracy-increases-throughout-2017-muso-reveals>, accessed 13 November 2020; Ofcom, 'Online Content Study', 14 March 2016, <https://www.ofcom.org.uk/research-and-data/technology/internet-wifi/online-content-study>, accessed 4 November 2020; ‖ Authors' video interview with a content protection agency, 17 July 2020; European Commission, 'Counterfeit and Piracy Watch List', p. 13; ¶ The majority of linking sites do not host infringing content directly. See ECLI:EU:C:2016:644, 'Judgment of the Court (Second Chamber)', 8 September 2016, <http://curia.europa.eu/juris/document/document.jsf?text=&docid=183124&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=10205240>, accessed 8 November 2020; ** European Commission, 'Counterfeit and Piracy Watch List', p. 9; †† Authors' video interview with an investigative member association, 11 August 2020.*

Note: This table draws on IPO, Online Copyright Infringement (OCI) Tracker*, 9th Wave (London: The Stationery Office, 2019); Europol and EUIPO, '2017 Situation Report on Counterfeiting and Piracy in the European Union', p. 31.*

Audio-Visual Piracy: Key Trends and Patterns

The way illegal content is distributed and consumed today bears little resemblance to even a decade ago, as shown by the timeline below. Compared to the monopoly held by peer-to-peer (P2P) services in the early 2000s, there are now a myriad of ways to distribute AV content illegally.

Access to infringing material is now instantaneous, with pirates capable of delivering a professionalised and slick service, often including the same on-demand and live channels as legitimate providers. Published in February 2020, the 9th Wave of the UK Intellectual Property

Office's (IPO) *Online Copyright Infringement (OCI) Tracker* concluded that around 25% of UK citizens used an illegal source to access some form of copyright-infringing content in 2019.[21] This number rose to 34% for live sports and 27% for films, representing an 8% rise in film infringement in 2019 compared to the previous year.[22] By contrast, the percentage of people consuming infringing TV programmes decreased from 23% in 2018 to 17% in 2019.[23] Promisingly, however, there was also a significant decrease in consumers who *only use illegal sources to access content* between 2018 and 2019, from 11% to 2% for film; 11% to 7% for music; and 14% to 2% for TV.[24] This decline in only accessing illegal content is likely because of the popularity and accessibility of legal on-demand IPTV services, such as Netflix, NowTV and Amazon Prime. Nonetheless, the OCI Tracker shows that piracy remains a significant source of AV content for a sizable amount of the UK population.[25]

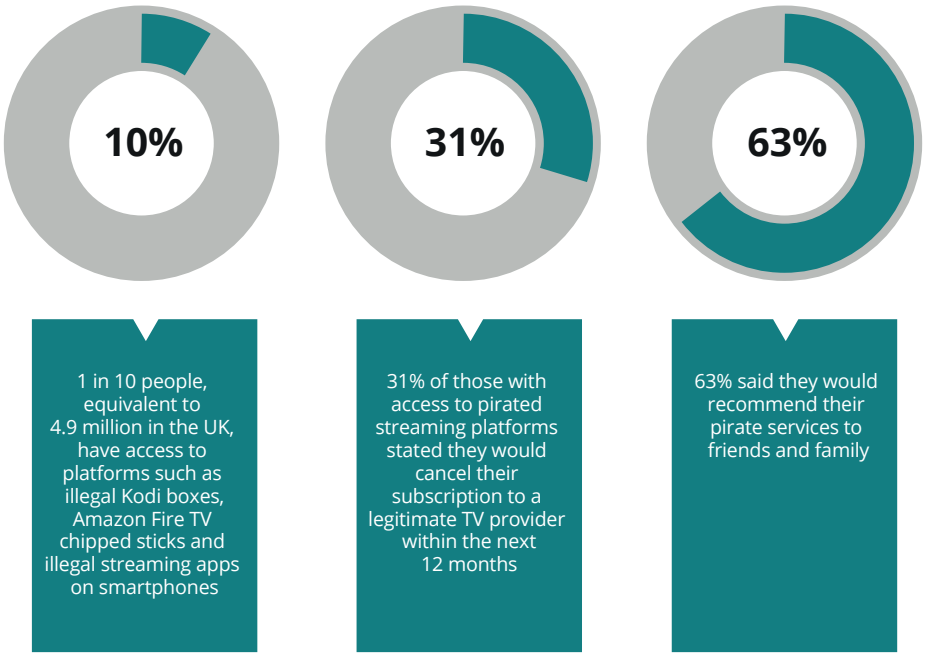
Although the OCI Tracker figures are a useful benchmark, especially given their comparability to previous annual 'waves' of the survey, they are not definitive. Consumer research performed by the Industry Trust – an industry-funded consumer education body with over 20 members – puts the average level of infringement in the UK at 37% of the population, significantly higher than the OCI Tracker's 25%.[26] Furthermore, a 2017 YouGov survey found that 1 in 10 of the UK population have access to platforms such as illicit streaming devices, 'cracked' Amazon Fire TV Sticks (which have been illegally modified from their original form by criminals), and illegal streaming apps on smartphones and tablets.[27] Almost a third (31%) of those with access to pirated streaming platforms stated they would cancel their subscription to a legitimate TV provider within the next 12 months.[28] Over 63% said they would recommend pirate services to friends and family.[29] According to MUSO, an IP consultancy, there were more than 190 billion visits to pirate sites in 2018 – with 5.85 billion visits from UK IP addresses.[30]

In 2020, PIPCU reported a rise in the number of people who are buying subscription services from illicit IPTV suppliers without also purchasing a hardware device.[31] Such subscriptions

21. IPO, *Online Copyright Infringement (OCI) Tracker*, 9th Wave (London: The Stationery Office, 2019). This figure is an aggregate of all content categories the OCI evaluates, including film, TV, music, live sports, video games, software and e-publishing. The estimate excludes digital images.
22. IPO, *Online Copyright Infringement (OCI) Tracker*, 9th Wave.
23. *Ibid*.
24. *Ibid*.
25. MUSO, 'Global Piracy Increases Throughout 2017, MUSO Reveals'.
26. IPO, 'IP Crime and Enforcement Report 2019-20', p. 71.
27. Russell Feldman, 'Almost Five Million Britons Use Pirated TV Streaming Services', YouGov, 20 April 2017, <https://yougov.co.uk/topics/politics/articles-reports/2017/04/20/almost-five-million-britons-use-illegal-tv-streami>, accessed 9 November 2020.
28. *Ibid*.
29. *Ibid*.
30. MUSO, 'Global Piracy Hits 190 Billion Visits in 2018, But UK Sees a Drop', <https://www.muso.com/magazine/global-piracy-hits-190-billion-visits-in-2018-but-uk-sees-a-drop>, accessed 3 February 2021.
31. IPO, 'IP Crime and Enforcement Report 2019-20', p. 45.

provide access to apps or services that can be used on smart TVs, smartphones, tablets and other devices, such as games consoles. This ease of access has played an important role in transforming the social acceptability of piracy and thus consumers' increasing willingness to pay for illegal pirate content. An Industry Trust survey of 2,257 UK-based adults (aged 18+) between December 2019 and January 2020 found that 31% currently pay to access infringing content via a box, stick or smart TV app, while 51% of infringers have never paid for infringing content.[32] A separate Industry Trust survey of 2,166 UK-based adults in June 2020 found that 31% of those surveyed 'who had ever infringed' (683) had paid a one-off or regular fee for an illicit subscription.[33]

Figure 1: The Impact of Pirated Streaming Services in the UK, March 2017



Source: Author generated. Based on YouGov, 'The Impact of Pirated Streaming Services in Britain', March 2017.

32. Industry Trust, 'Moments Worth Paying For Consumer Research', March 2020. Total sample size of 2,626 individuals comprised of 2,257 British adults (aged 16+) and 369 children aged 11–15. Statistics based on sample of all infringers aged 18+, excluding sports infringers only, n=789 individuals.
33. Industry Trust, 'Quarterly Tracker: Quarterly Research into the GB Population's Usage of, and Attitudes Towards, Infringement Methods', June 2020. Total sample size of 2,166 adults aged 16+. Based on 683 of 2,166 individuals who have ever paid for infringing content.

IP Crime is Organised Crime: Piracy, Organised Crime Networks and Individual Offenders

The criminals providing pirated content have proven consistently capable of adapting to and capitalising on social, technological and economic changes to accumulate profit and evade enforcement action. To date, however, piracy has not been prioritised as a profit-generating form of organised crime or cybercrime by law enforcement, academia or parts of industry, such as the financial sector.[34]

Organised Crime Networks vs Individual Offenders

There is a variety of actors who distribute pirated material for commercial gain, including individual criminals and organised crime networks.[35] Offender profiles appear to vary depending on the type of service they offer. According to PIPCU, individual offenders tend to operate illegal streaming websites and cyberlockers, while IPTV and subscription-based services are typically operated by OCGs.[36] This defies the commonly held perception that piracy is solely carried out by otherwise law-abiding, opportunistic individuals. Although OCGs are the higher law enforcement priority, individuals can also make significant criminal gain from piracy.[37] Furthermore, although disrupting an OCG can have a larger impact on the scale of criminality, it is also the case that disrupting individuals engaged in lower-level crime can generate intelligence to inform the disruption of common vulnerabilities in pirate business models and be time- and cost-effective. For example, PIPCU carries out face-to-face 'cease and desist' visits to lower-level offenders that often result in a halt to the criminal activity.[38]

Broadly speaking, however, it is doubtful whether lone operators have the resources and expertise required to maintain large-scale direct-hosting sites due to the complex, costly and time-consuming infrastructure involved.[39] Although individual criminals may be able to manage smaller hosting or linking sites, interviewees suggested that administrative complexity grows with the popularity of the site and postulated that the number of people involved in running a website-based piracy operation may grow in tandem with the volume of traffic and content.[40] A 2019 analysis of rogue cyberlockers also found 'a remarkably centralised system with just a few networks, countries and cyberlockers underpinning most provisioning', with many exhibiting high levels of HTML

34. Authors' interview with a foreign law enforcement official, 31 July 2020; authors' interview with two senior UK law enforcement officers, 13 August 2020; authors' interview with an international policy stakeholder, 3 September 2020; authors' interview with a rights holder, 8 July 2020.
35. Europol and EUIPO, '2017 Situation Report on Counterfeiting and Piracy in the European Union', p. 33.
36. Official data provided by PIPCU.
37. See, for example, PIPCU's investigation with the New York District Attorney's Office into an individual hacker operating from the UK in IPO, 'IP Crime and Enforcement Report 2019-20', p. 91.
38. Official data provided by PIPCU.
39. Authors' interview with two senior academics, 21 July 2020. The inverse may also be possible for highly technologically proficient individual operators.
40. Authors' interview with two senior UK-based academics, 21 July 2020.

similarity and operating based on shared domains and hosting facilities.[41] The authors of that 2019 report concluded that this small number of providers are proficient in evading law enforcement detection, sometimes even rebranding before relaunching if a site is taken down.[42] Further research is therefore needed on the extent to which the operators of hosting sites, linking sites and cyberlockers are run by the same OCGs.

In comparison, IPTV providers are typically hierarchical and well organised due to the technical knowledge and infrastructure required to provide consistent access to high-quality on-demand and live content.[43] Key figures in organised IPTV crime groups include the initial content providers, streaming infrastructure hosts, distributors and finally the resellers who offer packages directly to consumers (see Figure 2).[44] IPTV operations can generate significant amounts of criminal income. In March 2019, three UK-based men were sentenced to over 17 years' imprisonment for conspiracy to defraud after they earned more than £5 million from the sale of ISDs and online piracy since 2009.[45] Many groups operate transnationally: in June 2020, the Spanish National Police dismantled a criminal network supplying IPTV to an estimated two million customers across Europe, Asia and the Middle East, worth €15 million a year in profit (see Box 2).[46] A 2019 EUIPO study concluded criminal IPTV providers make nearly €1 billion a year supplying pirate content in the EU.[47] The average single user in the EU spent €5.74 per month on unauthorised IPTV, according to the same report.[48]

IPTV's growing dominance in the piracy landscape is made possible in part by the rise of 'piracy as a service' (PaaS). Using a PaaS model, organised crime networks can market and sell tools, programmes and expertise to new offenders to help them begin or improve the administration of their own piracy operations (see Box 1). This includes the ability to purchase professional-looking website templates and fully stocked content libraries, as well as 'middleware' or 'panel' providers

41. Damilola Ibosiola et al., 'Movie Pirates of the Caribbean: Exploring Illegal Streaming Cyberlockers', Association for the Advancement of Artificial Intelligence, 2018, <https://arxiv.org/pdf/1804.02679.pdf>, accessed 3 February 2021.
42. *Ibid*.
43. Official data provided by PIPCU; Europol and EUIPO, '2017 Situation Report on Counterfeiting and Piracy in the European Union'.
44. Official data provided by PIPCU.
45. FACT, 'Three Sellers of Illegal Streaming Devices Jailed for a Total of 17 Years for Defrauding Premier League', 21 March 2019, <https://www.fact-uk.org.uk/three-sellers-of-illegal-streaming-devices-jailed-for-a-total-of-17-years-for-defrauding-premier-league/>, accessed 9 January 2021.
46. Europol, 'Illegal Streaming Service With Over 2 Million Subscribers Worldwide Switched Off', press release, 10 June 2020, <https://www.europol.europa.eu/newsroom/news/illegal-streaming-service-over-2-million-subscribers-worldwide-switched>, accessed 10 January 2021.
47. EUIPO, *Illegal IPTV in the European Union: Research on Online Business Models Infringing Intellectual Property Rights – Phase 3* (Alicante: EUIPO, 2019), p. 10.
48. *Ibid*., p. 9.

who provide the app-based technology to deliver IPTV content to consumers.[49] In a 2019 study, Prakhar Pandey, Maxwell Aliapoulios and Damon McCoy suggest 'middleware' functionality can include software that enables subscriber management, reseller management, stream management, transcoding[50] and generating TV channel playlists.[51] Other middleware services include pre-made website templates with access to vast content libraries containing thousands of infringing TV and film titles. One open source investigation found 1,544 pirate sites using the same WordPress template, for example.[52] Some middleware allows the reseller to use a personal URL and design their own site branding, meaning multiple sites with the same beneficial owner may appear unconnected.

Those who sell IPTV subscription accounts via a middleware service are therefore referred to as 'resellers'. Resellers are crucial figures in the sale of IPTV subscriptions and fully loaded ISDs, but they are unlikely to personally know or have direct contact with the ultimate beneficiaries running and coordinating the IPTV service itself. Indeed, middleware can enable OCGs or individual offenders with little technological know-how to start an IPTV operation, with Pandey, Aliapoulios and McCoy noting that 'for some, middleware providers are the first step in their infrastructure'.[53] This lowers barriers to entry for new offenders and further blurs the line between the types or quality of services that can be offered by individual operators and OCGs. In 2017, Europol noted the number of operators providing illegal IPTV 'appears to be on the rise and this trend is expected to continue at an accelerated rate in the future'.[54] A total of 56 years of prison time has been handed out to 25 illegal IPTV suppliers between October 2017 and November 2020 in the UK.[55]

Although not at the top of the food chain, IPTV account resellers can still make a significant amount of money. One online forum visited by the authors sold bulk IPTV subscriptions for €5 per account, with individual logins to be resold to consumers for €15–25 per month.[56] Another popular IPTV service operating solely in Bitcoin boasted that resellers could make up to €10,000

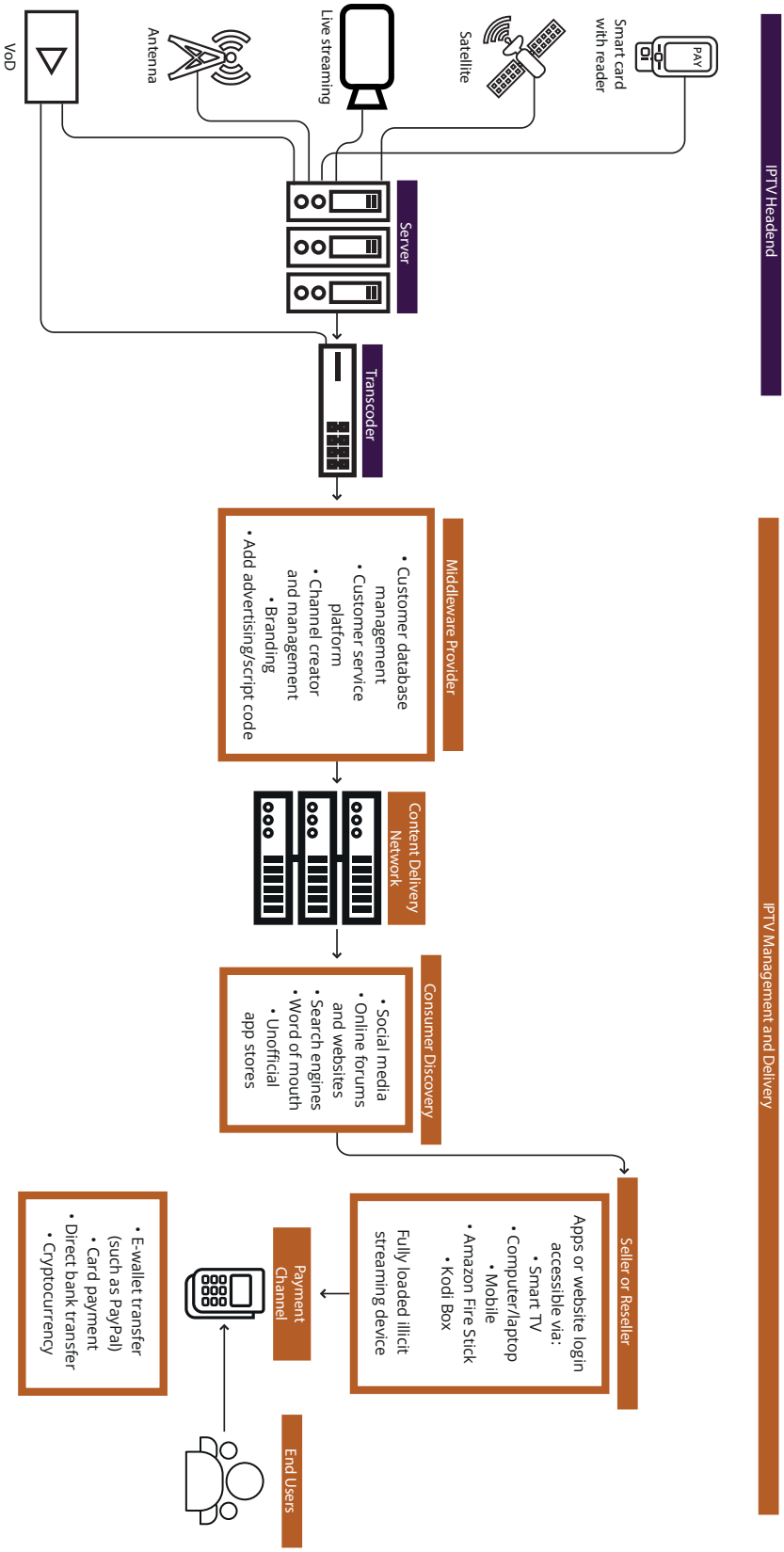
49. Prakhar Pandey, Maxwell Aliapoulios and Damon McCoy, 'Iniquitous Cord-Cutting: An Analysis of Infringing IPTV Services', 4th IEEE European Symposium on Security and Privacy Workshops, Stockholm, Sweden, 2019, pp. 423–32, <https://ieeexplore.ieee.org/abstract/document/8802514>, accessed 11 February 2021.
50. Transcoding is defined as the process of converting an audio or video file from one encoding format to another to increase the number of compatible target devices a media file can be played on. See Techopedia, 'Transcoding', last updated 31 October 2012, <https://www.techopedia.com/definition/973/transcoding>, accessed 7 November 2020.
51. Pandey, Aliapoulios and McCoy, 'Iniquitous Cord-Cutting', p. 432.
52. Primary data reviewed by the authors provided by the Alliance for Creativity and Entertainment (ACE)/Motion Picture Association (MPA).
53. Pandey, Aliapoulios and McCoy, 'Iniquitous Cord-Cutting', p. 432.
54. Europol and EUIPO, '2017 Situation Report on Counterfeiting and Piracy in the European Union', p. 32.
55. Data collected by FACT.
56. Online forum visited by the authors.

a month by upselling annual subscriptions priced at €44 per account.[57] Significant profits can also be made from the sale of 'fully loaded' ISDs. In April 2018, John Dodds was sentenced to four-and-a-half years in prison for conspiracy to defraud after selling hundreds of 'fully loaded' ISDs in pubs and clubs in northeast England, including electrically faulty devices.[58] Dodds hid cash in his house and further assets in his daughter's name, with the court issuing a confiscation order for £521,000 on his conviction.[59]

The evolution of the easily accessible PaaS marketplace mirrors the rise of 'cybercrime as a service' (CaaS), a term used to capture the fact that criminals now regularly buy and sell the tools and techniques needed to facilitate cyber-enabled crimes such as distributed denial-of-service (DDoS) cyber attacks, hacking services to access specific systems, and malware and fraud.[60] CaaS represents 'the increased professionalisation of the cybercrime threat landscape' and is considered one of the most pressing organised crime threats across the EU.[61] PaaS may be considered a type of CaaS because it involves the sale of cybercrime tools and technology that enables offenders with limited technical knowledge to run high-quality, large-scale pirate services they would otherwise likely be incapable of offering.

57. Illegal IPTV service website visited by the authors, 22 January 2021.
58. Andy Maxwell, 'Man Who Sold Pirate IPTV Must Pay £521,00 or Face Five More Years in Prison', *TorrentFreak*, 28 February 2020, <https://torrentfreak.com/man-who-sold-pirate-iptv-must-pay-521000-or-face-five-more-years-in-prison-200228/>, accessed 7 November 2020.
59. *Ibid*.
60. Europol, *IOCTA 2016: Internet Organised Crime Threat Assessment* (The Hague: Europol, 2016), p. 7.
61. Europol, 'IOCTA 2020: Internet Organised Crime Threat Assessment', 2020, p. 31; Europol, 'EU Policy Cycle: EMPACT', <https://www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact>, accessed 8 January 2021.

Figure 2: IPTV Distribution



Source: Adapted from Prakhar Pandey, Maxwell Aliapoulios and Damon McCoy, 'Iniquitous Cord-Cutting: An Analysis of Infringing IPTV Services', 4th IEEE European Symposium on Security and Privacy Workshops, Stockholm, Sweden, 2019, <https://ieeexplore.ieee.org/abstract/document/8802514>, accessed 11 February 2021.

The well-organised nature of many piracy operations is further evidenced by the scale and continuity of their transnational operations, ability to maintain complex technical infrastructures and the incorporation of back-up systems to build in resilience in case of enforcement action.[62] This is demonstrated by the speed with which pirates capitalised on the coronavirus pandemic. UK authorities noted a spike from the beginning of the lockdown in March 2020 in scam advertisements on illegal sites, and emails and text messages offering access to Netflix or Disney+ accounts for free or for a discounted price.[63] The opportunity for lucrative windfalls from people staying at home were enough to convince the app Popcorn Time – dubbed by the media as the 'Netflix of piracy' – to launch 'version 4.0' after its closure in recent years.[64] MUSO reported that traffic to illegal streaming and downloading sites increased by nearly 60% in March 2020.[65]

62. See, for example, Europol, 'Widely Used Illegal Streaming Platform Switched Off From Switzerland', press release, 11 November 2020, <https://www.europol.europa.eu/newsroom/news/widely-used-illegal-streaming-platform-switched-switzerland>, accessed 3 February 2021; Europol and EUIPO, *IP Crime and Its Link to Other Serious Crimes*.
63. Official data supplied by ACE/MPA.
64. Jason Koebler, 'Legendary Piracy App Popcorn Time Comes Back From the Dead During Coronavirus Pandemic', *VICE*, 17 March 2020.
65. *BBC News*, 'Coronavirus: Film Piracy Streaming Trebles in Lockdown', 15 May 2020.

Illegal IPTV operators used the coronavirus crisis as a platform to expand and legitimise their own services. Anticipating high consumer demand from the resumption of live football in summer 2020, pirates invested significantly in their infrastructure while also improving their ability to penetrate protection mechanisms used by rights holders (such as IP- and geo-blocking).[66] Pirates also adapted their advertising and marketing strategies. Research for this report found several examples where public health messaging and government guidelines were spun to encourage viewing illegal content as a way of fulfilling civic duties.[67] For example:

> Stay home, stay safe! … we are with you during the worldwide fight against the corona virus. Please follow guidance from public health officials and government agencies.
>
> …
>
> Code: COVID20 for 20% off. Stay safe at home.
>
> …
>
> Stay home, save lives.
>
> …
>
> For customers who will receive [our] package, we want to assure you that the packages sent go through a sterilisation and disinfection process. The process is performed by our delivery partner Amazon. Our packages are therefore completely secure.[68]

66. Synamedia, 'Post COVID-19 Effect: Rising Piracy Steals the Ball from Broadcasts of Returning Crowdless Football Matches', 25 June 2020, <https://www.synamedia.com/blog/post-covid-19-effect-rising-piracy-steals-the-ball-from-broadcasts-of-returning-crowdless-football-matches/>, accessed 14 November 2020.
67. Primary data reviewed by the research team provided by the ACE/MPA.
68. *Ibid*.

Box 1: Operation *Xtream Codes*: 22 Arrests Against Major Organised Crime Network Running Pan-European IPTV Service

On 18 September 2019, a multi-country operation coordinated by Eurojust dismantled an international organised crime network 'committing massive fraud' by providing IPTV. Eurojust said the incident 'shows organised crime expanding its illegal activities to large-scale violations of audiovisual copyright'.[*] Described as 'skilled criminals', Xtream Codes began providing IPTV in 2015 using 'the most sophisticated and efficient software [available] for the fraud'.[†]

Investigators arrested 22 suspects spread across France, Germany, Greece, Bulgaria and the Netherlands, taking down more than 200 servers and blocking over 150 PayPal accounts.[‡] Criminal damages were estimated to be approximately €6.5 million, putting 'thousands of jobs in danger' according to Filippo Spiezia, Italy's representative at Eurojust.[§] Xtream Codes was registered as a company in Bulgaria, had a local VAT number, and listed an address in Petrich for its offices. According to Eurojust, illegally obtained assets were subsequently transferred to foreign bank accounts.

Xtream Codes was one of the most prominent 'middleware' providers at the time, enabling prospective pirates to purchase a 'do-it-yourself' kit and launch their own pirate services. Its software package provided services such as transcoding, server and channel management, stream tracking and geo-blocking. The product was engineered to be extremely user-friendly, meaning that resellers did not require a high level of technological capability to be successful. Templates provided by Xtream Codes would allow resellers to customise their IPTV packages by setting up and renaming channels and adding logos. Resellers often advertised their packages on Facebook groups and other social media networks.[‖] An average subscription ranged between €15 and €49 a month, depending on the reseller.[¶]

Xtream Codes reportedly provided 'back-end management support' to over 5,000 IPTV apps, providing content to an estimated 50 million viewers.[**] Global illicit streaming traffic reportedly decreased by 50% in the days following the raid.[††] Suspects face charges including large-scale fraud, cybercrime and money laundering.

Sources: [*] EU Agency for Criminal Justice Cooperation (Eurojust), 'Eurojust Helps Unravel Massive Trans-European Pay-TV Fraud', press release, 18 September 2019, <https://www.eurojust.europa.eu/eurojust-helps-unravel-massive-trans-european-pay-tv-fraud#:~:text=A%20multi%2Dcountry%20action%20day,scale%20violations%20of%20audiovisual%20copyright>, accessed 4 November 2020; [†] Ibid.*; [‡] Europol and EUIPO,* IP Crime and Its Link to Other Serious Crimes*; [§] EURACTIV, 'European Police Smash "World's Largest" TV Piracy Operation', 19 September 2019, <https://www.euractiv.com/section/digital/news/european-police-smash-worlds-largest-tv-piracy-operation/>, accessed 13 November 2020; [‖]* Ibid.*; [¶] Andy Maxwell, 'Xtream Codes IPTV System Targeted in Massive Police Operation (Updated)',* TorrentFreak*, 18 September 2019, <https://torrentfreak.com/xtream-codes-iptv-system-targeted-in-massive-police-operation/>, accessed 13 November 2020; [**]* Sky News*, 'Police Raid "Network of Pay-TV Pirates" Broadcasting to Tens of Millions Worldwide', 18 September 2019; [††] Office of the USTR, '2019 Review of Notorious Markets for Counterfeiting and Piracy', 2019, p. 4, <https://ustr.gov/sites/default/files/2019_Review_of_Notorious_Markets_for_Counterfeiting_and_Piracy.pdf>, accessed 9 January 2021.*

Piracy and Poly-Criminality

Poly-criminal groups or individuals are those who engage in multiple crime types. As Chapter III explores in detail, malware, fraud and identity theft are the most well-evidenced forms of poly-criminality exhibited by pirates. These crimes are likely to generate a significant amount of revenue.

Recent Europol reports draw attention to the fact that 'piracy is often linked to cybercrime and identity fraud', and that 'OCGs involved in counterfeit goods and copyright infringements commonly use cash intensive businesses, including legitimate ones, to mix criminal and legitimate incomes'.[69] Money laundering – that is, the movement and use of criminal proceeds – is by necessity an 'indispensable element' of IP crime, including piracy.[70] The European Commission notes that the 'difference between legitimate cloud storage services and rogue cyberlockers is that cyberlockers usually mask the identity of their operators via domain privacy services and via offshore companies, which makes it hard for enforcement authorities to link these sites to any natural person',[71] which is also useful in laundering the funds. This is a further reason why improved KYBC rules are required to help identify the operators of pirate services, as discussed in Chapter III.

Although it is possible that some networks and groups do rely on professional money launderers, as a relatively low-priority crime for law enforcement, the majority of criminals involved in counterfeiting and piracy do not appear to outsource the financial or laundering elements to a third party.[72] In July 2018, for example, a UK-based couple were jailed for their role in the sale of over 8,000 ISDs worth £750,000 through a purpose-built website.[73] Investigations revealed several further offences, including the use of a shell company in Nevis in the Caribbean to launder the proceeds, as well as the immigration crime of providing false documents to sponsor an Egyptian national who maintained the illegal streaming service for the company.[74] In the UK, guidance issued by the Crown Prosecution Service encourages prosecutors to consider money-laundering charges in all IP crime cases, noting that almost all offences under the Trade

69. Europol and EUIPO, *IP Crime and Its Link to Other Serious Crimes*, p. 66.
70. Europol and EUIPO, '2017 Situation Report on Counterfeiting and Piracy in the European Union', p. 39.
71. European Commission, 'Counterfeit and Piracy Watch List', p. 9.
72. A professional money launderer specialises in the provision of money-laundering services, which can also be performed while acting in a legitimate, professional occupation. The Financial Action Task Force (FATF) provides guidance on the techniques used by such criminals. See FATF, 'Professional Money Laundering', July 2018, <www.fatf-gafi.org/media/fatf/documents/Professional-Money-Laundering.pdf>, accessed 3 February 2021.
73. Rob Kennedy and Katie Dickinson, 'Blyth Pirate Jailed for Illegally Streaming Premier League Football and Films', *ChronicleLive*, 16 July 2018.
74. FACT, 'Five Year Jail Sentence for Operator of Major Illegal Streaming Service', 16 July 2018, <https://www.fact-uk.org.uk/five-year-jail-sentence-for-operator-of-major-illegal-streaming-service/>, accessed 5 February 2021.

Marks Act 1994 and Copyright, Designs and Patents Act 1988 are Schedule 2 lifestyle offences.[75] Yet, as discussed below, this approach can be inaccessible when a case is pursued through private prosecution, which is the case for many IP crime cases in the UK.[76]

Notwithstanding their connections to money laundering, fraud and malware, there is little evidence that those involved in piracy systematically engage in violent or non-cyber-enabled offences. This stands in contrast to OCGs involved in counterfeiting, where there are well-established links to modern slavery, drug trafficking and human trafficking.[77] Interviewees were able to recount anecdotal examples where OCGs involved in piracy were also found to be engaging in drug trafficking, weapon trafficking and corruption, but systemic links were not proven.[78] This may be because investigations into IP crime offences do not focus on or attempt to identify other criminal activities carried out by the same group.[79] Where there have been attempts at bringing this information together, such as in the UK's annual IP crime and enforcement report,[80] it is usually not disaggregated across counterfeiting and piracy. These intelligence gaps impede law enforcement's understanding of the scale and impact of the harm from piracy alone.

75. Schedule 2 lifestyle offences are typically committed by criminals to acquire wealth. See Crown Prosecution Service (CPS), 'Intellectual Property Crime', last updated 8 November 2019, <https://www.cps.gov.uk/legal-guidance/intellectual-property-crime>, accessed 22 January 2021.
76. House of Commons Justice Committee, 'Private Prosecutions/Safeguards: Ninth Report of Session 2019–21', 2 October 2020, HC497, <https://committees.parliament.uk/publications/2823/documents/27637/default/>, accessed 7 February 2021; authors' interview with UK law enforcement investigator C, 2 February 2021.
77. Europol and EUIPO, '2017 Situation Report on Counterfeiting and Piracy in the European Union', p. 4; European Commission, 'Counterfeit and Piracy Watch List', p. 2; UN Office on Drugs and Crime, 'Focus On: The Illicit Trafficking of Counterfeit Goods and Transnational Organized Crime', <https://www.unodc.org/documents/counterfeit/FocusSheet/Counterfeit_focussheet_EN_HIRES.pdf>, accessed 8 November 2020.
78. Authors' interview with a content protection company, 15 July 2020; authors' interview with a content protection company, 17 July 2020; authors' interview with a UK law enforcement investigator, 20 July 2020; authors' interview with a non-UK rights holder, 22 July 2020; authors' interview with two UK policymakers, 31 July 2020; see also Box 2.
79. Authors' interview with enforcement representatives, 31 July 2020.
80. See IPO and IP Crime Group, 'IP Crime and Enforcement Report 2017/18', p. 13.

Box 2: Former Police Officer Coordinated Organised Crime Networks Involved in Drug Trafficking and IPTV Sales

In June 2020, Daniel Aimson – a former Greater Manchester Police officer – was sentenced to 12 months' imprisonment for selling 123,000 illegally loaded ISDs and further subscriptions to IPTV in 2016–17.[*] His sentence will be served consecutively because in 2017, Aimson was jailed for over six years for conspiracy to produce cannabis estimated to be worth £85,000 and misconduct in a public office.[†] His drug-trafficking operation involved at least seven known individuals who were also convicted.

Prosecutors said his 'sophisticated' operation selling IPTV 'Zgemma boxes' online made £655,000 in just 13 months. Devices and subscriptions were sold on eBay, Amazon, Twitter, LinkedIn and other sites. Working with three others, he accrued at least £300,000 in criminal income in one merchant bank account between January and August 2017.[‡] Payments were also made by PayPal and into a bank account in the name of his wife at the time.

Demonstrating best practice, the case was investigated and pursued by the Federation Against Copyright Theft (FACT) after they were alerted by Barclaycard, who initially provided a card payment service on the operation's website.[§]

Sources: [*] Chris Slater, 'Ex-Cop Who Lived Life of Luxury with Wife Until He Was Jailed for Drugs Conspiracy is Sentenced AGAIN… This Time for Selling TV Boxes with Illegal Software', Manchester Evening News*, 2 June 2020. Note, the group sold more than 123,000 ISDs via eBay but only this number were proven to be illegally loaded. This reduced the estimated damages to broadcasters in the case significantly; [†]* BBC News*, 'Greater Manchester Police Officer in Leigh Drugs Gang Jailed', 20 December 2017; [‡] None of this income was declared to Her Majesty's Revenue and Customs Service. See Slater, 'Ex-Cop Who Lived Life of Luxury with Wife Until He Was Jailed for Drugs Conspiracy is Sentenced AGAIN… This Time for Selling TV Boxes with Illegal Software'; Andrew Bardsley, '"It Was Easy Money": GMP Car Cleaner Lured in by Cop Turned Drugs Boss',* Manchester Evening News*, 17 June 2020; [§] FACT, 'Seller of Illegal Devices That Bypassed Paid-For TV Content Has Been Jailed', 2 June 2020, <https://www.fact-uk.org.uk/seller-of-illegal-devices-that-bypassed-paid-for-tv-content-has-been-jailed/>, accessed 13 November 2020.*

Policy and Enforcement Implications

Many experts feel that the increased professionalisation and involvement of organised crime networks in piracy calls for greater enforcement action. A more 'multi-nodal, multi-sectoral, multi-jurisdictional' approach is required to tackle piracy, according to one policy expert.[81] Others noted that the scale and harm of the crime triggers the application of the '4Ps' of organised crime policing: to **pursue** offenders; to **protect** individuals, systems and organisations from the effects of organised crime; to **prepare** for when organised crime occurs and mitigate

81. Authors' interview with a US policymaker, 7 August 2020.

impact; and to **prevent** people from engaging in serious and organised crime (SOC).[82] In the piracy ecosystem context, this means:

- **Pursue**: Requires a holistic enforcement approach, executed through a combination of disruption, investigation and prosecution activities. Disruption is focused on ways to frustrate the operation of criminal activities, whether this entails administrative site blocking, technical measures to degrade the quality of online streams, or arrangements with financial institutions to identify and block activity connected to pirate operations. Identifying and locating offenders wherever they may be, with a view to prosecuting individuals or groups and recovering illicit assets, forms the rest of the 'pursue' approach.
- **Protect**: There are two main facets to this in the context of AV piracy. The first concerns the need to educate individual consumers on the risk of engaging in piracy in terms of malware, hacking and fraud. The second relates to the impact of piracy on the creative industries, whose business models and ability to grow and maintain staff is threatened by piracy.
- **Prepare**: The 'prepare' function in this context is designed to ensure rights holders and law enforcement are adequately positioned to mitigate the harm of copyright infringements at the point at which they occur. It also refers to certain defensive mechanisms designed to protect copyrighted material. This includes technical measures such as 'watermarking' technology which is designed to identify which device the infringement is coming from and allow rights holders to deactivate the pirated device.[83]
- **Prevent**: There is an urgent need to deter people from engaging in the distribution of pirated material for personal financial gain. This is particularly relevant given the rise of PaaS, which lowers barriers to entry for new offenders. Prevention also includes people who have been recruited as money mules and 'cammers' of newly released films.[84] There is also a need to deter consumers from paying for and consuming pirated material, as discussed in Chapter III.

Current Enforcement Landscape

The current enforcement landscape for piracy-related crimes in the UK contains a broad mix of public and private sector stakeholders who need to work together in a whole-of-system approach to tackle piracy. These organisations and some of their roles in enforcing and protecting IP rights are detailed in Table 2.

82. Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS), '4P', <https://www.justiceinspectorates.gov.uk/hmicfrs/glossary/4p/>, accessed 6 November 2020.
83. Authors' interview with a content protection agency, 15 July 2020; authors' interview with a UK-based broadcaster, 30 July 2020.
84. 'Camming' refers to the act of recording films using a handheld device in a cinema or theatre. See IPO, 'IP Crime and Enforcement Report 2019–20', 2020, p. 44.

Table 2: Key Enforcement Stakeholders

Organisation	Role
PIPCU (City of London Police)	PIPCU has responsibility for investigating and deterring serious and organised IP crime in the UK, protecting consumers from harms which may arise from it.[*]
Intellectual Property Office (IPO)	The IPO is the UK government body responsible for IP rights including patents, designs, trademarks and copyright. They are responsible for IP policy, educating businesses and consumers about IP rights and responsibilities, supporting IP enforcement and granting UK patents, trademarks and design rights.[†]
National Trading Standards and local Trading Standards chapters	Trading Standards authorities have responsibility for enforcing criminal IP legislation, including the Copyright, Designs and Patents Act 1988. They are responsible for investigating and gathering intelligence around the country to combat fraud, counterfeiting and rogue traders.[‡]
National Economic Crime Centre (NECC)	The NECC is the central point of coordination for the UK's response to economic crime, bringing together public and private sector intelligence and capabilities.[§] The NECC coordinates the activities of the Joint Money Laundering Intelligence Taskforce (JMLIT), a public–private partnership that exchanges operational information and typologies.
Regional Organised Crime Units (ROCUs)	There are 10 ROCUs across England and Wales which provide local police forces with access to a standardised set of capabilities to help their work against serious organised crime. These specialist capabilities may include cybercrime or fraud investigations.[‖] ROCUs are also home to Regional Economic Crime Units, including Regional Asset Recovery Teams (RARTs) and Regional Cyber Crime Units.
Local police forces	Local police forces have responsibility for policing IP crime at the local level (e.g. the sale of counterfeit goods in physical marketplaces) and coordinating with relevant agencies to obtain or provide information pertinent to an investigation.

Organisation	Role
Crown Prosecution Service (CPS)	The CPS has a duty to take over police IP prosecutions when notified of a case by the police. It also provides legal guidance and advice relevant to stakeholders around thresholds for investigation and prosecution.[¶]
Investigative member associations (e.g. FACT)	Investigative member associations provide a range of services and strategic and tactical solutions designed to tackle crime and support businesses. Core business areas include due diligence and verification, forensics and intelligence, online investigations and legal services.[**]
Content monitoring/protection services	These offer services which help Pay-TV operators, rights holders and broadcasters control the distribution of legitimate content. They also provide protection for live and non-live content across broadcast and 'over-the-top' (OTT) services.
Broadcasters/rights holders	Broadcasters and rights holders may monitor online marketplace listings and removals of items used in connection with piracy. They may detect infringements by keyword searches and use of logos and trademarks.[††]
Content owners	Activities may include, among other things, monitoring, disrupting and removing unauthorised content online, initiating private prosecutions, passing intelligence onto member associations and police forces, and collaborating with stakeholders to share intelligence and raise awareness around IP crime.
International law enforcement (e.g. Europol, Interpol)	International law enforcement facilitates and coordinates cross-border investigations and takedowns of criminal networks involved in IP crime. They have a role in monitoring and reporting crime trends and enhancing standardisation of legal instruments and operating procedures to counter IP crime globally.[‡‡]

Organisation	Role
Financial institutions	Financial institutions are obliged by law to report suspicious activities related to money laundering, namely the use of criminal proceeds, including the proceeds of IP crime. These obligations come to the fore when banks provide acquiring services that enable their customers to accept card payments. If a bank does not understand its customer's business, it risks processing payments for illicit goods or services, such as the provision of pirated AV content. The financial sector – including banks and payment service providers – can also refuse to initiate payments when their customers ask them to process payments to groups that run infringing websites.
Online advertising sector	The advertising sector includes all parties involved in placing, buying, selling and/or facilitating advertising. They are largely unregulated, but several voluntary codes of conduct, including a European Commission MOU and a programme coordinated by the Trust and Accountability Group, an industry association, exist to prevent advertising revenue monetising pirate services.

*Sources: * City of London Police, 'About PIPCU', <https://www.cityoflondon.police.uk/police-forces/city-of-london-police/areas/city-of-london/about-us/about-us/pipcu/>, accessed 14 November 2020; † IPO, 'About Us', <https://www.gov.uk/government/organisations/intellectual-property-office/about#our-responsibilities>, accessed 14 November 2020; ‡ National Trading Standards, 'About National Trading Standards', <https://www.nationaltradingstandards.uk/what-we-do/>, accessed 14 November 2020; § NCA, 'National Economic Crime Centre', <https://www.nationalcrimeagency.gov.uk/what-we-do/national-economic-crime-centre>, accessed 21 January 2021; ‖ HM Inspectorate of Constabulary (HMIC),* Regional Organised Crime Units: A Review of Capability and Effectiveness *(London: HMIC, 2015); ¶ CPS, 'Intellectual Property Crime'; ** IPO and IP Crime Group, 'IP Crime and Enforcement Report 2018–19', p. 63; †† Europol, 'Intellectual Property Crime Coordinated Coalition – IPC3', <https://www.europol.europa.eu/about-europol/intellectual-property-crime-coordinated-coalition-ipc3>, accessed 14 November 2020.*

Note: Some categories overlap. For example, the BBC is a rights holder, broadcaster and content owner. Some organisations may have additional roles in combating IP crime.

Challenges to Enforcement

The coordination of these diverse actors is challenging, an issue compounded by increasingly professionalised and sophisticated piracy operations.[85] In the UK context, it is particularly difficult to assess the true scale of IP crime due to the lack of a centralised reporting mechanism. It is also unclear whether IP-related crime detected in the course of the investigation of other offences is accurately recorded and intelligence shared among law enforcement agencies.[86] The absence of a single shared intelligence system accessible to all UK agencies with a role in policing IP crime compounds this issue and affects tasking for enforcement activities. This may change if piracy is integrated as a priority into the SOC System Tasking project, which will deliver a single, systematic and agreed approach to tasking across the SOC system.[87] Currently, there is also no official understanding of the extent and volume of poly-criminality or networked connections among offenders engaged in IP crime in the UK.[88] This data gap extends to victims, including those defrauded or exposed to fraud, malware and identity theft through digital piracy in the UK. Intelligence about this is likely to be spread across Action Fraud, Trading Standards, PIPCU, the Citizens Advice Bureau, the IPO and policing agencies, among others.

Interview data suggested that many rights holders therefore feel there is an inadequate level of prioritisation of piracy-related crimes and resources are still disproportionately focused on counterfeiting because the involvement of organised crime networks is better understood.[89] One interviewee emphasised that 'it should tick all the boxes which mean[s] that law enforcement sit up and take notice. There are no taxes being paid, people are involved in other criminality like money laundering [and] there's potential and probable harm to the consumer as well'.[90]

85. Authors' interview with two senior UK law enforcement officers, 13 August 2020. This is also commonly felt across Europe, although the exact agencies involved differ by country. See European Commission, 'Counterfeit and Piracy Watch List', p. 7; Europol and EUIPO, '2017 Situation Report on Counterfeiting and Piracy in the European Union', pp. 4, 43.
86. Authors' interview with a UK policymaker, 1 November 2020.
87. National Crime Agency (NCA), 'Leading the UK's Fight to Cut Serious and Organised Crime: Annual Plan 2019-20', p. 58, <https://nationalcrimeagency.gov.uk/news/nca-publishes-annual-plan-2019-20>, accessed 21 February 2021.
88. Trading Standards offers an annual breakdown of links found in their investigations in the IP Crime and Enforcement Report. See IPO and IP Crime Group, 'Trading Standards Successes: IP Crime and Enforcement Report 2019/20', 2020, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/913651/trading-standards-successes.pdf>, accessed 11 February 2021.
89. Authors' interview with a senior academic, 24 July 2020; authors' interview with a rights holder, 8 July 2020; authors' interview with a content protection company, 11 August 2020; IPO, 'IP Crime and Enforcement Report 2019-20', p. 6. See also Frontier Economics, 'The Economic Impacts of Counterfeiting and Piracy', 2016.
90. Authors' interview with an industry investigator, 11 August 2020.

However, neither the UK National Strategic Assessment for Serious and Organised Crime[91] nor the National Police Chiefs' Council Strategic Policing Requirements[92] mention piracy. Likewise, although cybercrime is a priority for EU organised crime policing, the 2020 Internet Organised Crime Threat Assessment makes no reference to piracy.[93]

Some interviewees attributed this to a lack of education or misconceptions about the volume of revenue and involvement of organised crime networks in piracy, while others felt that the novelty of some of the modern forms of piracy has made it easier to ignore and instead focus on crime areas with a traditional response framework.[94] Furthermore, the unwillingness of some online service providers and financial sector intermediaries to cooperate with law enforcement and rights holders in combating piracy – as discussed in Chapter III – was largely seen as motivated by their prioritisation of profit over consumer safety.[95]

Others noted that without an appreciation of these connections, law enforcement efforts will remain skewed towards individual, mid- and low-level resellers, allowing the more sophisticated, profitable and resilient OCGs to continue to flourish.[96] It is clear, for example, that while Trading Standards must continue to target resellers of illegal ISDs, they are not equipped, mandated or resourced to conduct higher-level organised crime or cybercrime investigations. Indeed, most piracy investigations require digital media and financial investigation skills and resources that are beyond the scope of individual local police forces, reinforcing the need for secondments, dedicated funding streams to target IP crime and greater coordination across the public sector to ensure investigations are correctly tasked and pursued. PIPCU's creation in 2013 and the IPO Intelligence Hub have contributed significantly to introducing this capability, but rights holders and law enforcement representatives feel more could be done when it comes to priority-setting at the higher levels of the policing infrastructure to ensure IP crime – and piracy in particular – are better represented.

IP crime requires a whole-of-system approach that coordinates agencies across government and activates investigative skills across the UK SOC policing network. This report does not promote a specific solution, but notes that some stakeholders suggested the IPO Intelligence Hub could play a greater role in coordinating action across law enforcement and government agencies

91. See NCA, 'National Strategic Assessment of Serious and Organised Crime 2020', April 2020, <https://www.nationalcrimeagency.gov.uk/who-we-are/publications/437-national-strategic-assessment-of-serious-and-organised-crime-2020>, accessed 9 January 2021.
92. See Home Office, 'The Strategic Policing Requirement', March 2015, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/417116/The_Strategic_Policing_Requirement.pdf>, accessed 9 January 2021.
93. Europol, 'IOCTA 2020', p. 31; Europol, 'EU Policy Cycle'.
94. Authors' interview with a rights holder, 7 July 2020; authors' interview with a content protection company, 17 July 2020; authors' interview with a rights holder, 20 July 2020.
95. Department of Homeland Security, 'Combating Trafficking in Counterfeit and Pirated Goods', Report to the President of the United States, 24 January 2020.
96. Authors' interview with former UK law enforcement officers, 24 February 2020.

to address IP crime.[97] This includes intelligence sharing across law enforcement partners such as PIPCU, Trading Standards, local police forces and the 10 ROCUs across England and Wales to ensure that specialist capabilities in areas like cybercrime, financial investigation and fraud are available to pursue IP crime cases. As it stands, IP crime currently lacks the necessary prioritisation and intelligence sharing is too decentralised. A whole-of-system response could also seek to increase coordination across the broader UK public sector on IP crime, bringing in agencies with a hitherto underdeveloped role in targeting piracy and counterfeiting. For example, the Financial Conduct Authority and the NECC, the UK's central point of coordination for the economic crime response, prioritise fraud and money-laundering issues writ large but do not consider IP crime, despite its high-grossing nature.

A fundamental part of achieving this more networked SOC-based response is an appreciation of the transnational nature of piracy operations. Piracy investigations often demand not only specialist investigation skills, but also cooperation with foreign law enforcement agencies. Updated in December 2020, the European Commission's Counterfeit and Piracy Watch List features numerous examples of pirate sites hosted and operated from multiple countries, including one cyberlocker hosted in Germany but suspected to be operated from Switzerland; and another hosted in Switzerland but operated from Russia.[98] The operators of Popcorn Time, a popular piracy app mentioned above, are reportedly based in North Africa; as are the operators of other large-scale IPTV services.[99] Very few large-scale piracy operations are limited to one country, as further demonstrated by the variety of cases discussed throughout this report.

This transnational dimension presents a significant investigative challenge. The European Commission notes that illegal IPTV's ubiquitous footprint 'is the result of cooperation of illegal operators from various countries, making it difficult to find out the identity and precise location of an IPTV operator'.[100] Yet, although the majority of physical hosting infrastructure is located outside the UK, many online service providers, such as hosting intermediaries who are known to provide services to pirate operators, are based in Europe.[101] Maintaining the resources and relationships necessary to cooperate with international law enforcement counterparts is therefore a priority for IP crime investigations, particularly now the UK has left the EU.[102]

The reliance on internet technology and intermediary services means that pirates can be based anywhere in the world. This is a further reason why financial disruption is an important strategy. Even perpetrators based overseas rely on financial infrastructure or other legitimate intermediaries based in the UK and cooperative jurisdictions, which creates opportunities to introduce friction in their business model and use financial investigations to uncover and bring

97. Feedback received in IP and law enforcement validation workshop, 18 February 2021.
98. European Commission, 'Counterfeit and Piracy Watch List'.
99. *Ibid*.
100. *Ibid.*
101. Authors' interview with UK law enforcement investigators A and B, 12 August 2020; IPO, 'IP Crime and Enforcement Report 2017–18', p. 42; hosting provider data reviewed by the authors.
102. Authors' interview with a UK policymaker, 25 August 2020.

to justice the higher echelons of organised pirate networks. This is particularly important in tackling pirate groups operating from jurisdictions that are unlikely to cooperate with UK law enforcement agencies, as discussed in Chapter III.

Box 3: Worldwide IPTV Operation Grossing €15 Million a Year Shut Down in June 2020

In June 2020, the EU law enforcement agencies dismantled an IPTV network with over two million subscribers, generating at least €15 million in illegal profit a year.

The service provided over 40,000 TV channels and on-demand content. It also offered sophisticated technical assistance and quality control through a bespoke customer support platform.

Demonstrating the scale of the international operation, law enforcement authorities across the EU arrested 11 individuals across Spain, Germany, Sweden and Denmark, interrogating 16 others for their possible involvement in the illegal scheme.

The operation seized around €4.8 million in illicit assets, including properties worth more than €2 million, four cars worth about €500,000, luxury watches, cash, cryptocurrencies and electronic equipment. Law enforcement authorities took down 50 IP addresses and servers across Europe. A further 11 bank accounts totalling €1.1 million were also frozen.

Source: Europol, 'Illegal Streaming Service With Over 2 Million Subscribers Worldwide Switched Off', 10 June 2020, <https://www.europol.europa.eu/newsroom/news/illegal-streaming-service-over-2-million-subscribers-worldwide-switched>, accessed 10 January 2021.

II. Revenue Models

THIS CHAPTER ANALYSES how organised criminal networks generate revenue from the common distribution models outlined in Chapter I, including advertising and direct payments via the formal financial system. It also assesses the nascent role of crypto-assets[103] and cryptomining.[104] Finally, it outlines how income derived from other criminal activity including malware, fraud, identity theft and tax evasion is inseparable from the IP offence itself. Payment methods are analysed in detail so that financial institutions may better understand their exposure to risk from piracy.

These categories have been chosen to explore the characteristics and role of each revenue stream, but in reality, criminals are profit maximisers, and most groups will seek as many forms of monetisation as possible. Piracy operations with multiple sources of revenue also have increased resilience if one source is disrupted.[105] Although there are non-monetary benefits and motivations for offenders running illegal piracy operations,[106] the vast majority of organised crime networks and individuals are motivated by profit. A 2015 study funded by the Motion Picture Association and carried out by Incopro – a content protection consultancy – concluded that at least 91.6% (570) of the 622 most popular hosting, linking and public P2P sites in Germany, Spain, Italy, France and the UK had at least one source of revenue (see Figure 4).[107] Sites with no obvious monetisation were generally the least popular according to Alexa rankings, with the exception of some notable outliers in Germany.[108]

Advertising is likely to remain a primary form of raising revenue from online traffic because it is compatible with almost every content distribution model and can be combined with other tactics such as malware and direct payments. Incopro's 2015 analysis demonstrates that

---

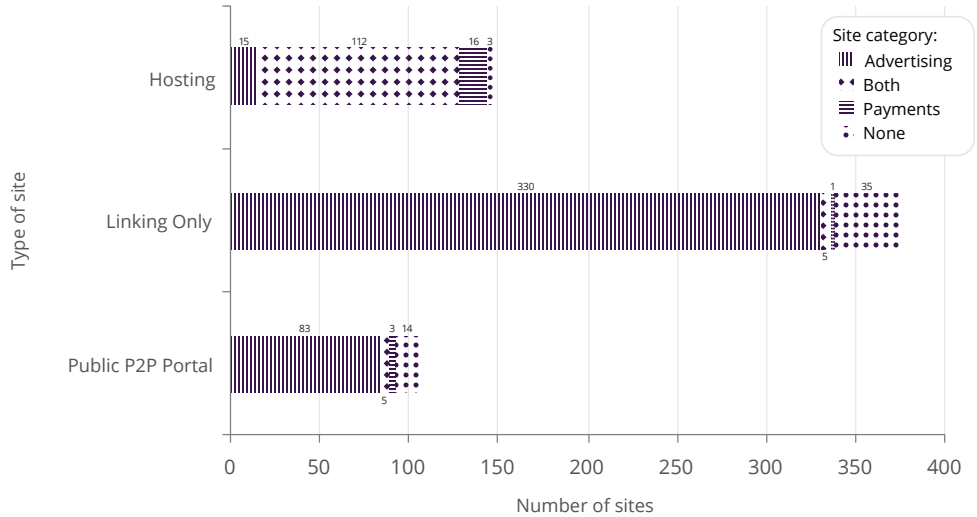
103. Crypto-assets (used interchangeably with cryptocurrency) are cryptographically secured digital representations of value or contractual rights that can be transferred, stored or traded electronically. All crypto-assets use some form of distributed ledger technology (DLT).
104. Cryptomining is a process in which transactions for various forms of cryptocurrency are verified and added to the blockchain digital ledger. Each time a transaction is made, a miner is responsible for ensuring the validity of the information and updating the blockchain with the transaction.
105. Incopro, 'The Revenue Sources for Websites Making Available Copyright Content Without Consent in the EU', 2015, p. 27.
106. Authors' interview with an industry association representative, 8 July 2020. See also OECD, *Piracy of Digital Content* (Paris: OECD, 2009).
107. Incopro, 'The Revenue Sources for Websites Making Available Copyright Content Without Consent in the EU', 2015, p. 9. Although conducted in 2015, this remains one of the most comprehensive and in-depth studies of hosting, linking and public P2P sites conducted for the EU.
108. Incopro, 'The Revenue Sources for Websites Making Available Copyright Content Without Consent in the EU', p. 9.

hosting sites are most likely to combine direct payments and advertising revenue, while linking and P2P are predominantly sustained by advertising only.[109] Many platforms use 'freemium' models characterised by a mixture of subscription- and advertising-based content, similar to legitimate business models like YouTube or Spotify. According to the EUIPO, paid upgrades offer the user perks such as faster download speeds and multiple file downloads at the same time if they create an account with personal credentials or buy a time-limited package.[110] This is also common across cyberlockers, hosting sites and apps.[111] MegaUpload, a major organised crime group indicted by the US in 2012, was funded through a combination of premium access (estimated $150 million in revenue) and advertising (estimated $25 million).[112]

As discussed below, there is no agreed formula for estimating criminal revenue from subscription- or advertising-funded piracy. This report demonstrates, however, that criminal income earned from piracy moves through the formal financial system on a regular basis. Cyberlockers also warrant more attention in this regard, as they often directly reward users for uploading their own infringing content.[113] This can be done either monetarily or in credits that can be used for their own access to the site. The European Commission records that rewards offered to users depend on the size of the downloaded file, the location of the downloader and the number of times the content was downloaded or streamed.[114] A 2014 NetNames and Digital Citizens Alliance report found 70.6% of cyberlockers' revenue comes from premium accounts and 29.4% from advertising, with the 15 largest direct-download cyberlockers making $63.1 million in annual revenue, or around $4.2 million per site every year.[115]

109. *Ibid*., p. 11.
110. Francesca Bosco and Andrii Shalaginov, 'Identification and Analysis of Malware on Selected Suspected Copyright-Infringing Websites', EUIPO, September 2018.
111. European Commission, 'Counterfeit and Piracy Watch List'.
112. US v. Kim Dotcom, Megaupload Limited, Vestor Limited, Finn Batato, Julius Bencko, Sven Echternach, Mathias Ortmann, Andrus Nomm and Bran Van Der Kolk, Indictment, 2012, <https://www.scribd.com/document/78786408/Mega-Indictment>, accessed 10 January 2021.
113. Ellen Seidler, 'Cyberlockers: Explaining Piracy's Profit Pyramid', Pop Up Pirates, 15 December 2011, <https://popuppirates.com/what-i-know-pyramid-of-piracy-profits/>, accessed 10 January 2021; European Commission, 'Counterfeit and Piracy Watch List'.
114. European Commission, 'Counterfeit and Piracy Watch List'; infringing sites visited by the authors.
115. Digital Citizens Alliance and NetNames, 'Behind the Cyberlocker Door: A Report on How Shadowy Cyberlocker Businesses Use Credit Card Companies to Make Millions', 2014, <https://fia-actors.com/fileadmin/user_upload/News/Documents/2014/Oct/dca-netnames-cyber-profibility-ph11.pdf>, accessed 4 February 2021.

Figure 3: Revenue Sources for Top 622 Unauthorised Sites



Source: Incopro, 'The Revenue Sources for Websites Making Available Copyright Content Without Consent in the EU', 2015.

Payment Methods

Advertising

Advertising is the largest and most common source of funding for pirate services, chiefly because it offers a quick, relatively anonymous and often lucrative method of monetising a site. Some 'middleware' providers even offer a script that can be installed by the site operator that will enable the site to place adverts with minimal effort, rapidly monetising even the newest operations.[116] The European Commission notes that advertising 'in many cases is the sole reason that pirate services can continue to operate'.[117] An in-depth understanding of how advertising revenues made through pirate sites are transferred to their operators and then integrated within the broader financial system remains an intelligence gap for law enforcement.[118]

There are multiple advertising mediums used to monetise pirate sites. Commissioned by the EUIPO, White Bullet suggests the most common types of advertisements are: pop-up ads; pop-under ads; mid-page units; skyscrapers (vertical at the sides of a page); and banners (horizontal at the top of the page).[119] Adverts can be static or mobile and might also include

116. Authors' interview with a former UK law enforcement investigator, 24 February 2020.
117. European Commission, 'Counterfeit and Piracy Watch List', p. 21.
118. Authors' interview with UK law enforcement investigator C, 2 February 2021.
119. White Bullet Solutions Limited ('White Bullet'), *Digital Advertising on Suspected Infringing Websites* (Alicante: EUIPO, 2016), pp. 10, 17, <https://euipo.europa.eu/ohimportal/

in-text partner affiliate links and promo codes. Payment for advertising might be rewarded through combinations of views, pay-per-clicks and other traceable actions, as well as a standard fee decided through bidding for ads.[120]

There is currently no agreed formula for estimating how much an advertisement is worth on a pirate site, which complicates the act of estimating total criminal revenue from piracy.[121] Some estimates of the value of an advert on a pirate site vary from $0.30 to $2.50 per 1,000 viewer impressions.[122] Reaching an accurate estimate is complicated by the fact that different types of advertising generate different volumes of revenue, with a video worth more than a static image, and a premium brand worth more than a non-household name, for example.[123]

In 2021, White Bullet estimated the 1,000 most popular pirate sites visited by UK consumers make up to £37 million a year from advertising; the top 10 of these are estimated to make £12 million. This rises to £460 million made by those same websites when including revenue streams from other countries.[124] By contrast, some older studies arrive at much higher valuations. For example, the Digital Citizens Alliance – an industry-funded US non-profit organisation – estimated that the top 596 piracy sites generated a combined $227 million in advertising revenue in 2013, with the top 30 sites earning an average of $4.4 million annually.[125] A follow-up study of a cohort of similar sites a year later found this fell

---

documents/11370/80606/Digital+Advertising+on+Suspected+Infringing+Websites>, accessed 11 February 2021.

120. Google, 'Understanding Bidding Basics', <https://support.google.com/google-ads/answer/2459326?hl=en-GB>, accessed 6 November 2020; BASCAP, 'Roles and Responsibilities of Intermediaries: Fighting Counterfeiting and Piracy in the Supply Chain', March 2015, p. 76; Digital Citizens Alliance and Risk IQ, 'Digital Bait: How Content Theft Sites and Malware are Exploited by Cybercriminals to Hack into Internet Users' Computers and Personal Data', December 2015, p. 6.
121. Authors' interview with a UK law enforcement investigator, 12 September 2020; authors' interview with a UK law enforcement investigator, 11 September 2020; authors' interview with a UK law enforcement investigator, 21 September 2020; authors' interview with a non-UK law enforcement policy official, 31 July 2020.
122. Digital Citizens Alliance, 'Good Money Still Going Bad: Digital Thieves and the Hijacking of the Online Ad Business', May 2015, <https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/goodstillbad.pdf>, accessed 10 January 2021; Ernst and Young, 'Measuring Digital Advertising Revenue to Infringing Sites', September 2017, <https://www.tagtoday.net/hubfs/Measuring%20digital%20advertising%20revenue%20to%20infringing%20sites.pdf?t=1507150221706>, accessed 10 January 2020.
123. Interactive Advertising Bureau, '2021 Marketplace Outlook', 15 December 2020, <https://www.iab.com/insights/2021-marketplace-outlook/>, accessed 10 January 2021.
124. White Bullet, <https://www.white-bullet.com/about-ipip>, accessed 19 February 2021. White Bullet provides research services to the EUIPO, mainly focused on advertising revenue from digital piracy.
125. Digital Citizens Alliance, 'Good Money Gone Bad: Digital Thieves and the Hijacking of the Online Ad Business', February 2014, <https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/good-money-gone-bad.pdf>, accessed 10 January 2021.

to an estimated $209 million in illegal advertising revenue in 2014.[126] Finally, a study funded by the Trustworthy Accountability Group (TAG) – a voluntary advertising industry initiative to combat criminal activity – estimated the top 672 pirate sites in the US generated $111 million in ad revenue in 2016, the majority of which (83%) came from non-premium advertisers such as gaming, dating and virtual private network (VPN) services.[127]

As will be discussed in Chapter III, the advertising marketplace is extremely complex, involving many intermediaries. According to White Bullet's evaluation of the impact of the European Commission's 2018 MOU with advertising intermediaries, a total of 4,752 unique ad intermediaries served 2,545,062 adverts across 7,627 'monitored websites' in 2019.[128] At least 3,847 unique brands were still identified on high-risk or illegal sites, including 546 unique named 'major brands'.[129] Just over half (52%) of all branded advertising was from the gambling sector, with 20% identified as 'Arts and Entertainment', including gaming.[130] Although the UK Gambling Commission has taken strong action to tackle gambling advertising on pirate sites, discussed below, gambling advertisements remain a persistent global funding source for pirate websites.[131]

Other studies further demonstrate the fragmentation of the marketplace and the need for a broad coalition of actors to stem the flow of advertising to pirate sites. In their 2015 analysis, Incopro profiled 3,544 adverts on 622 infringing sites in total, delivered by 279 unique advertising intermediaries, with no single ad intermediary responsible for delivering a greater proportion of ads against other networks.[132] Three intermediaries accounted for 34% of adverts by volume, with the top 10 intermediaries delivering 61% of total adverts served.[133] They found trick button advertisements and malware to be the most prevalent form of advertising on pirate sites, followed by gambling and adult content.[134]

---

126. Digital Citizens Alliance, 'Good Money Still Going Bad'.
127. Ernst and Young, 'Measuring Digital Advertising Revenue to Infringing Sites'.
128. Monitored websites are those identified as being either 'illegal websites' or 'high risk websites' according to the European Commission's terms of reference. See European Commission, *Study on the Impact of the Memorandum of Understanding on Online Advertising and Intellectual Property Rights on the Online Advertising Market* (Luxembourg: Publications Office of the European Union, 2020), p. 7.
129. European Commission, *Study on the Impact of the Memorandum of Understanding on Online Advertising and Intellectual Property Rights on the Online Advertising Market*, p. 6.
130. *Ibid*., p. 4.
131. Group-IB, 'Jolly Roger's Patrons', July 2020, p. 5; authors' interview with two senior academics, 21 July 2020; authors' interview with a non-UK rights holder, 22 July 2020; authors' interview with an international policymaker, 6 August 2020; authors' interview with a non-UK-based content protection agency, 16 June 2020.
132. Incopro, 'The Revenue Sources for Websites Making Available Copyright Content Without Consent in the EU', p. 13.
133. Incopro, 'The Revenue Sources for Websites Making Available Copyright Content Without Consent in the EU'.
134. *Ibid*.

Direct Payment

Direct payment for pirate services has become more common with the rise of IPTV but is also seen on cyberlockers and hosting sites.[135] As outlined in Table 1, direct payments may be made once for an illegally loaded ISD or on an ongoing basis for access to high-quality app-based or streaming subscription services.

In 2020, PIPCU projected a reduction in hardware sales and a rise in subscription-based piracy models, which indicates a rise in direct payment methods for infringing content.[136] Nonetheless, physical devices remain popular and a significant volume of ISD sales still occur in cash at physical marketplaces and shops.[137] This is seen to be declining, with sellers preferring the anonymity provided by online websites, social media and third-party e-commerce platforms. Amazon, eBay and Facebook formally banned the sale of ISDs in 2017,[138] and rights holders confirm there are far fewer blatant sellers on online marketplaces now due to the proactive measures that have been taken by platforms and content owners, with sellers having to rely on misspelled or obscure key words in their listings. This introduces some friction, but test purchases by rights holders confirm ISDs are still available for purchase online.[139] In 2019, the Digital Citizens Alliance published evidence of illegally loaded ISDs sold on dark web marketplaces.[140]

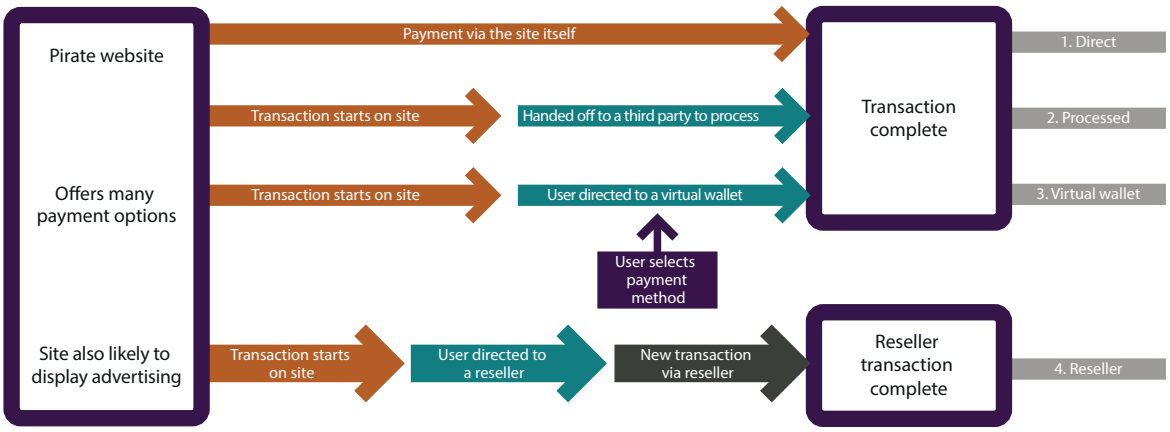
It is difficult to accurately estimate how much money is expended on piracy via direct payment by a consumer. Average direct spend on unauthorised content by consumers surveyed by the Industry Trust in 2019 varied but increased by an average of £12 between November 2018 and February 2019. In February 2019, those who paid one-off fees spent an average of £48, with 8% paying over £100. In the same time period, those who paid an ongoing fee spent an average of £60 per year, with 17% paying over £100.[141]

Incopro's 2015 analysis found that almost one in four sites (142 of the 622 sites analysed) offered direct payment methods, while the remaining three in four sites did not accept payment through the means originally advertised.[142] One-third of the 108 test purchases made as part of the analysis were completed through the requested payment method, with the remaining

135. IPO, 'IP Crime and Enforcement Report 2019-20', p. 45.
136. *Ibid*.
137. Incopro, 'The Revenue Sources for Websites Making Available Copyright Content Without Consent in the EU'.
138. FACT, 'Facebook Bans the Sale of Illicit Streaming Devices', 25 May 2017, <https://www.fact-uk.org.uk/facebook-bans-the-sale-of-illicit-streaming-devices/>, accessed 10 January 2021.
139. *Ibid*.
140. Digital Citizens Alliance, 'Fishing in the Piracy Stream: How the Dark Web of Entertainment is Exposing Consumers to Harm', April 2019, p. 12.
141. Industry Trust, 'Illicit Streaming Device Quarterly Tracker: Quarterly Research into the GB Population's Awareness, Usage of, and Attitudes Towards Illicit Streaming Devices (ISDs)', February 2019.
142. Incopro, 'The Revenue Sources for Websites Making Available Copyright Content Without Consent in the EU', p. 21.

transactions completed by third-party processing, a virtual wallet or a reseller.[143] This is significant because the mere presence of a legitimate payment intermediary logo may not mean those facilities are actually available.

Figure 4: Direct Payment Infrastructure

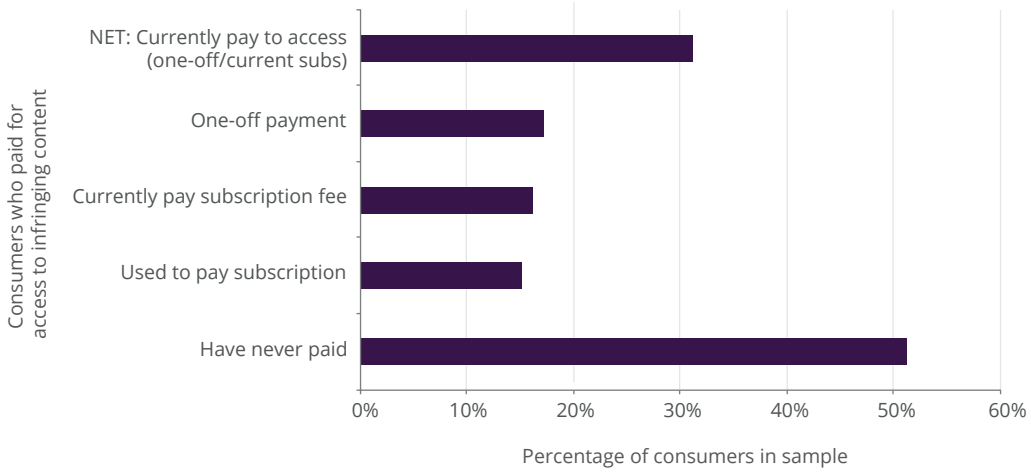


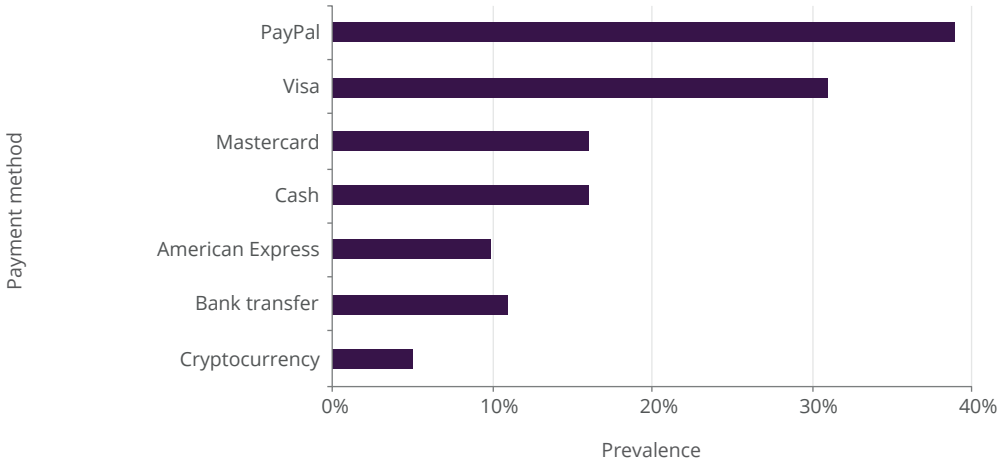
Source: Adapted from Incopro, 'The Revenue Sources for Websites Making Available Copyright Content Without Consent in the EU'.

Nonetheless, it remains the case that piracy is still often paid for through well-known payment processors. The Industry Trust's March 2020 consumer survey data showed a variety of payment methods used by the 31% who paid to access infringing content via a box, stick or smart TV app, including PayPal (39%), Visa (31%), Mastercard (16%), cash (16%), American Express (10%), direct bank transfer (11%), and cryptocurrency (5%).[144] Incopro's earlier study revealed similar results, but with a much broader range of payment intermediaries. Incopro broadly categorised payment methods into: payment schemes such as Visa and MasterCard; payment processors such as Liqpay and Dalpay; virtual wallets such as Google Wallet, RoboKassa and PayPal; and resellers such as VIPKeys (see Figure 5).[145] This is important because the ability to conduct transactions through the same payment providers consumers use to make various other legitimate everyday payments may lead some to conclude a service is legitimate or their personal and payment data is secure.

143. *Ibid*., p. 4.
144. Industry Trust, 'Moments Worth Paying For Consumer Research', March 2020. The total sample size of 2,626 individuals comprised of 2,257 British adults (aged 16+) and 369 children aged 11–15. Statistics based on a sample of all infringers aged 18+, excluding sports infringers only, n=789 individuals. See Figure 6.
145. Incopro, 'The Revenue Sources for Websites Making Available Copyright Content Without Consent in the EU', p. 28.

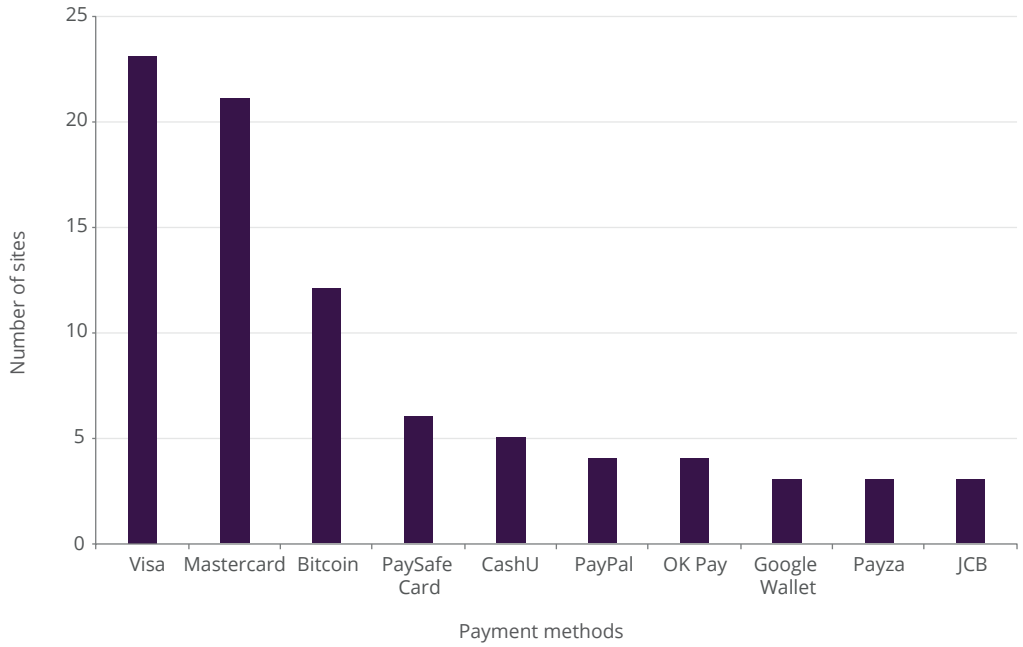
Figure 5: Consumers Who Pay for Access to Infringing Material





Source: Industry Trust, 'Moments Worth Paying For Consumer Research', March 2020.

Figure 6: Payment Methods and Test Purchases



Source: Incopro, 'The Revenue Sources for Websites Making Available Copyright Content Without Consent in the EU'. Sample of 622 infringing sites in Germany, Spain, Italy, France and the UK.

Law enforcement intelligence suggests that payment methods vary depending on the size of the piracy operation. While smaller or individual operators are more likely to accept payment via personal accounts using well-known providers such as PayPal, larger operations are likely to establish registered companies and merchant accounts.[146] Sometimes these companies are a mere front for illegal activity, but many companies also engage in legal trade – particularly those involved in the sale of illegal ISDs and counterfeit goods.[147] Law enforcement and financial investigators working on IP crime expressed frustration at the difficulty of distinguishing between illicit and licit profits when funds are co-mingled.[148] The use of companies is common and introduces complexity for financial institutions attempting to separate legitimate and illegitimate activity related to merchant accounts, as will be explored in Chapter III.

146. Authors' interview with a UK law enforcement investigator, 21 July 2020; authors' interview with a UK law enforcement investigator, 24 July 2020.
147. Authors' interview with an industry association, 20 July 2020; authors' interview with a UK law enforcement investigator, 21 July 2020; authors' interview with a UK law enforcement investigator, 24 July 2020; BASCAP, 'Roles and Responsibilities of Intermediaries', p. 12; Europol and EUIPO, '2017 Situation Report on Counterfeiting and Piracy in the European Union', p. 41.
148. Authors' interview with a UK law enforcement investigator, 28 August 2020; authors' interview with a UK law enforcement investigator, 21 July 2020.

The rise of direct payments for pirate services should be cause for concern for financial institutions who service criminal clients and transactions. It may be argued that many high-profile, well-known financial intermediaries are aware of this risk because of their reactive role in responding to rights holders' complaints, yet this issue is not currently prioritised by the sector. The majority of those interviewed for this research noted that the financial sector does not seem to proactively address piracy, and collaboration is based on personal relationships, which creates inequitable access for smaller, less well-resourced businesses seeking to protect their IP.[149] Current interventions are explored from Chapter III onwards.

Fundraising Through Other Criminal Activities: Malware and Identity Theft

Pirates also make money from other types of organised crime, including malware, fraud and identity theft. These crimes may be more lucrative when traditional advertisement or direct payment revenue is high, because they depend on high subscription or visitors to the pirate service itself.

These crimes are intimately connected to advertising revenue through 'malvertising', which refers to embedded malicious or otherwise unwanted programmes within advertisements that provide a way to spread malware using legitimate marketing platforms.[150] A 2016 report commissioned by the EUIPO found 51% of advertisements present on their infringing website list contained malware.[151] An earlier 2015 report by the Digital Citizens Alliance found that one out of every three websites that distributed copyright-infringing films and TV contained malware, with over half (55%) of malware infections traced back to user-initiated downloads, with the remaining 45% downloaded as a background process in so-called 'drive-by downloads'.[152]

A 2018 study commissioned by the EUIPO of malware on copyright-infringing sites found the use of a number of deceptive techniques and social engineering tools, such as empty game installations and adverts for free 'useful' software, to encourage users to initiate downloads of potentially unwanted programmes (PUPs).[153] Most PUPs were benign but designed to encourage users to input their personal details or sensitive information.[154] Multiple PUPs reviewed by the study provided end-user licence agreements that granted permissions such as the right to modify user accounts, access the internet, modify and delete files on an SD card, read phone

149. Authors' interview with a financial institution, 14 July 2020; authors' written correspondence with a financial institution, 17 July 2020; authors' interview with a non-UK-based content protection agency, 16 June 2020; authors' interview with a content protection agency, 17 July 2020; authors' interview with a non-UK law enforcement policy official, 31 July 2020.
150. Bosco and Shalaginov, 'Identification and Analysis of Malware on Selected Suspected Copyright-Infringing Websites', p. 10.
151. White Bullet, *Digital Advertising on Suspected Infringing Websites*, p. 23.
152. Digital Citizens Alliance and Risk IQ, 'Digital Bait', p. 6.
153. Bosco and Shalaginov, 'Identification and Analysis of Malware on Selected Suspected Copyright-Infringing Websites', p. 10.
154. *Ibid*., p. 3.

identities and access phone logs, contacts and device cameras.[155] PUPs were discovered for Microsoft Windows, Android and Mac systems, suggesting that 'the malware developers try to affect as many users as possible by using different platforms'.[156] No 'profoundly harmful' malware such as ransomware or botnets were found, but the study concluded 'the threat landscape for malware distributed via copyright-infringing websites is more sophisticated than it might appear at first glance'.[157]

There are no independent figures of what percentage of UK consumers of infringing content go on to experience malware, fraud, hacking or identity theft as a direct result of accessing pirate services. Industry Trust consumer survey data from June 2020 suggests 21% of all those who had ever infringed had experienced hacking, with a further 29% experiencing a virus or malware, and 7% becoming a victim of fraud as a result of hackers obtaining personal information.[158] Eight percent of those who had ever infringed reported their personal identity had been compromised or they had lost files or data stored on their device.[159] Crimestoppers extrapolates these figures to find that: 3.395 million illegal streamers were infected with viruses in 2019; 1.482 million had their personal details copied; 1.347 million were hacked; and 926,836 had money stolen online due to illegal streaming.[160] These figures are useful but they cannot be used to prove that consumers were affected as a direct result of accessing infringing content. An accurate understanding of UK consumers affected by fraud as a result of piracy is again impeded by the lack of a centralised reporting mechanism for IP crime.[161]

To date, a combination of lenient social attitudes towards piracy and intermediaries, such as search providers, hosting companies and online service providers who have maintained a lax approach to piracy have enabled pirates to operate openly on the surface internet.[162] The dark web, nonetheless, plays a potentially important role in supporting the criminal revenue models employed by pirates. In 2017, Europol and EUIPO flagged that although still comparatively limited, the dark web is increasingly used to share entire media databases and illegally retrieved

155. *Ibid*., pp. 48–57.
156. *Ibid*., p. 18.
157. *Ibid*., p. 57.
158. Industry Trust, 'Quarterly Tracker'. Total sample size of 2,166 adults aged 16+. Statistics are based on a sample size of 1,792 individuals who 'watch unauthorised films/TV/sport through apps and addons used on devices'.
159. *Ibid*.
160. Crimestoppers, 'Streaming Online – Know the Risks', <https://crimestoppers-uk.org/keeping-safe/online-safety/streaming-online-know-the-risks>, accessed 13 November 2020. This includes all who illegally stream through a modified box, stick, add-on or app.
161. Authors' interview with a UK policymaker, 21 July 2020; authors' interview with two senior UK law enforcement officers, 13 August 2020.
162. See also Department of Homeland Security, 'Combating Trafficking in Counterfeit and Pirated Goods', pp. 11, 26.

access codes to legitimate subscription services in particular, allowing unauthorised access to large libraries of IPR-protected films, music and other media.[163]

It is unclear, however, to what extent valuable personal data collected by the operators of infringing sites is resold online via the dark web, or if it is used by them directly for criminal gain.[164] This speaks to the difficulty of accurately identifying how malware or malvertising becomes embedded in pirate sites or to what extent website operators directly defraud their customers. It is difficult to conclusively prove malware is placed there by the site operators themselves and it is possible, for example, that some piracy sites may be hacked by external malicious actors and malware embedded without the knowledge of the website operators.[165] Moreover, it was pointed out by interviewees that malware may be less prominent in IPTV-subscription piracy models because of the need for repeat custom, and that some organised criminal networks would be wary of undermining their business model.[166]

Finally, many piracy services or tutorials online recommend the use of VPNs that may themselves pose a security risk to users by granting a wide range of permissions including the right to repurpose users' IP address as an exit node for other VPN activities.[167] This means, for example, that a user's IP address could be used to access pornography and underage content without their permission. The OCI Tracker demonstrates that a significant portion of UK-based infringers use a VPN.[168] Further evidence is required, however, to demonstrate that the VPNs marketed to infringers are intentionally malicious.

Cryptomining and Crypto-Assets: A New Trend

The use of crypto-assets for direct payments and cryptomining as a piracy revenue model has been observed in multiple European law enforcement investigations, a trend PIPCU predicts will increase.[169] One European law enforcement agent observed that pirate sites will offer a

163. Europol and EUIPO, '2017 Situation Report on Counterfeiting and Piracy in the European Union', p. 30.
164. Authors' correspondence with Andrii Shalaginov, 27 October 2020.
165. *Ibid*.
166. Authors' interview with a representative of an industry member association, 16 June 2020; authors' interview with an academic, 13 July 2020.
167. Muhammad Ikram et al., 'An Analysis of the Privacy and Security Risks of Android VPN Permission-Enabled Apps', Proceedings of the 2016 Internet Measurement Conference, November 2016, pp. 349–64, <http://dx.doi.org/10.1145/2987443.2987471>, accessed 2 November 2020; Trend Micro, 'Shining a Light on the Risks of HolaVPN and Luminati', 18 December 2020, <https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/shining-a-light-on-the-risks-of-holavpn-and-luminati>, accessed 2 November 2020; authors' interview with a content protection agency, 15 July 2020; authors' interviews with two ISP representatives, 4 and 24 August 2020.
168. IPO*, Online Copyright Infringement (OCI) Tracker*, 9th Wave.
169. IPO, 'IP Crime and Enforcement Report 2019-20', p. 45; authors' interviews with two ISP representatives, 4 and 24 August 2020. See also Digital Citizens Alliance, 'Fishing in the Piracy Stream', p. 17.

20–30% discount for those who pay in crypto-assets, presumably because it decreases their risk of detection.[170] The Industry Trust's March 2020 consumer survey data showed 5% of infringers in the survey used cryptocurrency to pay for pirate material.[171]

Both legitimate and illegal streaming websites have also attempted to use cryptomining as a revenue stream. Legitimate examples include US TV streaming platform Showtime and even the UN Children's Fund (UNICEF).[172] Since 2017, the well-known piracy site, The Pirate Bay, has experimented with cryptomining as a revenue stream, justifying the decision in an administrator blog that states: 'We really want to get rid of all the ads. But we also need enough money to keep the site running'.[173] Nonetheless, users' reaction to this move was mixed, with some expressing concern that the code ran without the 'explicit knowledge or authorisation of users'.[174]

All three of the above examples chose to run CoinHive, a Javascript plug-in that forced visitors' devices to use their computing power to 'mine' for a cryptocurrency called Monero while they were on the site.[175] This is attractive to websites attempting to generate passive revenue from high traffic or long visits, such as when torrenting or consuming hours of film or TV content.

As a 'privacy coin', Monero also offered criminal sites like The Pirate Bay a further benefit by shielding both the addresses and amounts sent, received and held by users.[176] By comparison, better known cryptocurrencies, such as Bitcoin and Ethereum, operate on transparent blockchains which enable transaction volumes and addresses to be seen by anyone in the world,

170. Authors' interview with a foreign law enforcement policy official, 31 July 2020.
171. Industry Trust, 'Moments Worth Paying For Consumer Research'.
172. Showtime was heavily criticised for introducing the function without warning website users, while Unicef, by contrast, transparently asked users to opt in to assist in mining as a form of charitable donation. See Alex Hern, 'Ads Don't Work So Websites Are Using Your Electricity to Pay the Bill', *The Guardian*, 27 September 2017; Stan Higgins, 'Reports: Showtime Websites Used to Secretly Mine Cryptocurrency', Coindesk, 27 September 2017, <https://www.coindesk.com/reports-showtime-websites-used-secretly-mine-cryptocurrency>, accessed 25 October 2020; Kristin Houser, 'You Can Now Donate to Unicef by Mining Cryptocurrency', World Economic Forum, 2 May 2018, <https://www.weforum.org/agenda/2018/05/you-can-now-donate-to-unicef-by-mining-cryptocurrency>, 20 October 2020.
173. The Pirate Bay, Blog Post '242', not reproduced.
174. *BBC News*, 'Visitors "Help" Pirate Bay Mine Virtual Cash', 18 September 2017.
175. Krebs on Security, 'Who and What Is Coinhive?', 26 March 2018, <https://krebsonsecurity.com/2018/03/who-and-what-is-coinhive/>, accessed 14 November 2020.
176. Monero, 'What is Monero (XMR?)', <https://www.getmonero.org/get-started/what-is-monero/>, accessed 14 November 2020; Anton Moiseienko and Kayla Izenman, 'From Intention to Action: Next Steps in Preventing Criminal Abuse of Cryptocurrency', *RUSI Occasional Papers* (September 2019); FATF, '12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers', June 2020, p. 17, <https://www.fatf-gafi.org/media/fatf/documents/recommendations/12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf>, accessed 4 February 2021.

including law enforcement.[177] The criminal abuse of crypto-assets presents challenges to law enforcement and regulators, as demonstrated in Chapter III.[178]

Notwithstanding the shutdown of the CoinHive plug-in in March 2019, cryptomining is likely to remain attractive as a revenue model, chiefly because requiring customers to pay in crypto-assets (as opposed to using their computing power for cryptomining without their knowledge) can be alienating or confusing to infringing consumers who may not know what crypto-assets are or who associate the term with criminal activity.[179] A 2019 survey by the UK's Financial Conduct Authority of 2,132 UK consumers found that 73% did not know what a 'cryptocurrency' was or were unable to define it.[180] Multiple experts interviewed for this research noted that while crypto-assets may put off some infringers, many consumers have a reasonably high level of technological understanding, as evidenced by the widespread use of VPNs and installation of ISDs.[181] Consumer reactions to requests for payment to access pirate services via crypto-assets requires greater monitoring in the future.

177. See also Kayla Izenman, 'Crypto at the Crossroads: Exploring the Impact of the US Treasury's Bitcoin Sanctions', RUSI Commentary, 2 January 2019; RUSI and ACAMS, 'Cryptocurrency Risk & Compliance Survey', 2020, <https://www.acams.org/en/ACAMS-RUSI-Crypto-Survey-Report>, accessed 25 October 2020.
178. Authors' interview with a UK law enforcement investigator, 12 August 2020.
179. Authors' interview with a former UK law enforcement officer, 19 March 2020; authors' interview with a rights holder, 15 July 2020; authors' interview with a UK policymaker, 21 July 2020; authors' interview with legal counsel for a rights holder, 8 July 2020; authors' interview with an ISP, 4 August 2020; authors' interview with a content protection company, 17 July 2020.
180. Financial Conduct Authority (FCA), 'FCA Reveals Findings from First Cryptoassets Consumer Research', 7 March 2019, <https://www.fca.org.uk/news/press-releases/fca-reveals-findings-first-cryptoassets-consumer-research>, accessed 23 October 2020.
181. Authors' interview with two senior academics, 21 July 2020; IPO, *Online Copyright Infringement (OCI) Tracker*, 9th Wave; authors' interview with a non-UK law enforcement policy official, 31 July 2020.

III. The Role of Financial Disruption in Tackling IP Crime

THIS CHAPTER OUTLINES the role of financial disruption in addressing online piracy. It explains why it is essential that there is proactive action to disrupt the journey from illegal content distribution to cashing out the proceeds of crime. It starts with an examination of the roles of commercial intermediaries that may be unwittingly involved in facilitating piracy, including regulatory and other incentives they have to detect IP crime.

To provide a well-rounded view of how financial disruption can be used against the business models identified earlier, it discusses a range of possible strategies, which include: reducing advertisement on infringing websites; impeding access to infringing websites; disrupting payments for infringing content; improving financial investigation and the enforcement response to piracy; and reducing individual user demand for infringing content using financial information.

Advertisement Disruption

Dissuading businesses from placing advertisements on infringing websites is a vital means of tackling piracy. As mentioned in Chapter II, a distinction can be drawn between websites that sell advertising space and those that promote specific partners via 'affiliate' programmes. In the former case, legitimate companies may unwittingly find themselves advertising through infringing websites but can educate themselves to prevent this. Inadvertent placement may happen due to the intermediation of ad distribution networks who look for the most popular advertising venue without reference to the activity of the site. In the latter instance, the infringing website is working in partnership with advertisers or brands who wish to knowingly promote their materials or services on pirate sites, often including gambling websites.

The first significant effort aimed at curbing advertising on infringing websites was a certification programme for ad networks run by the Interactive Advertising Bureau (IAB).[182] With the IAB's support, the US Intellectual Property Coordinator and several major ad networks[183] adopted 'a set of best practices to address online infringement by reducing the flow of ad revenue to operators of sites engaged in significant piracy and counterfeiting'.[184] At present, the flagship initiative directed against advertising on infringing websites is the TAG, which shares threat

182. IAB, 'IAB CCPA Compliance Framework for Publishers & Technology Companies', <https://www.iab.com/guidelines/ccpa-framework/>, accessed 14 November 2020.
183. Including 24/7 Media, Adtegrity, Condé Nast and SpotXchange.
184. Victoria Espinel, 'Coming Together to Combat Online Piracy and Counterfeiting', White House Blog, 15 July 2013, <https://obamawhitehouse.archives.gov/blog/2013/07/15/coming-together-combat-online-piracy-and-counterfeiting>, accessed 14 November 2020.

intelligence and provides certification for companies that wish to verify the integrity of their digital advertising.[185]

As discussed in Chapter II, a 2018 European Commission MOU now brings together advertisers, ad agencies, trading desks, ad platforms, ad networks, ad exchanges for publishers, sales houses, publishers and IPR owners to share information and commit to stop ad placements on known infringing sites. White Bullet's 2019 evaluation of the MOU found a decrease in the proportion of ads collected from premium household name brands that are based or headquartered in the EU, falling from 93% to 75% in the first six months of 2019.[186] While positive, the same evaluation found the need to incorporate a broader range of advertising intermediaries to achieve greater effect. A similar advertising-focused MOU has been signed in Russia.[187]

In 2016, the UK Gambling Commission, in cooperation with PIPCU, took sector-focused action to combat this by issuing License Condition 16, informing gambling companies that '[you] must ensure that you do not place digital advertisements on websites providing unauthorised access to copyrighted content and must take all reasonable steps to ensure that third parties with whom you contract do similar[ly]'.[188] While this is positive, the Gambling Commission's influence on pirate advertising is hampered by the limited influence it has on non-UK gambling outlets that offer services to UK customers illegally in breach of the UK's licensing requirements. A further challenge is posed by very active rogue quasi-gambling outfits such as 1xBet, who embed their logos and advertisements as frames in the video itself (as opposed to a banner on a website, for example).[189]

Engagement with the advertising industry has spurred the creation of lists of infringing websites. PIPCU's world-leading Infringing Websites List (IWL) is disseminated across the advertising industry. The same principle underlies the World Intellectual Property Organization's 'WIPO Alert' platform, a list of over 3,400 websites that is likewise intended to inform advertisers about where they should not place their ads.[190] A disadvantage of such lists is the time it takes

185. Trustworthy Accountability Group (TAG), 'What is TAG?', <https://www.tagtoday.net/aboutus/>, accessed 14 November 2020.
186. 'Name brands' are 'major brands', also known as 'household brands'; White Bullet, 'White Bullet's Programme with the EU Commission is Moving the Dial to Success', 24 August 2020, <https://www.white-bullet.com/our-programme-with-the-eu-commission-is-moving-the-dial-to-success>, accessed 4 February 2021.
187. Group-IB, 'Russian Online Piracy Market Falls for the First Time in 5 Years', 1 November 2019, <https://www.group-ib.com/media/piracy-market-collapses/>, accessed 14 November 2020.
188. Gambling Commission, 'Advertising/Marketing Rules and Regulations', <http://www.gamblingcommission.gov.uk/for-gambling-businesses/Compliance/General-compliance/Social-responsibility/Advertising-marketing-rules-and-regulations.aspx>, accessed 4 February 2021.
189. Andy Maxwell, '1XBET: The Bizarre "CAM" Brand That Movie Pirates Love to Hate', *TorrentFreak*, 26 May 2019, <https://torrentfreak.com/1xbet-the-bizarre-cam-brand-that-movie-pirates-love-to-hate-190526/>, accessed 8 January 2021; Group-IB, 'Jolly Roger's Patrons'.
190. WIPO, 'WIPO Alert', <https://www.wipo.int/wipo-alert/en/>, accessed 4 February 2021.

to update them, which is why some content protection companies offer dynamically updated infringing website lists that take account of the new websites that are being created all the time. Conversely, PIPCU's IWL has the benefit of ensuring fairness in that those included on the list are given an opportunity to respond and each inclusion on the list is manually made by PIPCU. These programmes are effective but there is a long way to go, and very few financial intermediaries such as banks appear to use these lists to inform compliance activities. According to White Bullet, in 2019, 71% of ads on the highest-risk IP-infringing streaming sites in the UK were for branded campaigns, including premium household names.[191]

Some interviewees argued that Google could use its position in the advertising industry to greater effect in preventing online piracy besides refusing to show advertisements that relate to pirated content.[192] One of the means used by organised crime networks to attract consumers to infringing websites is by using Google Analytics to understand the main sources of internet traffic to their websites.[193] It is reportedly possible for Google to use Google Analytics IDs and/or Google Tag Codes to identify websites that are being run by the same person – even if the identity of that person remains unknown – and, in some instances, ascertain who is paying for advertising on those websites.[194] There appears to be no existing regulatory basis in the UK or the US to require Google to proactively look for this information and report it to law enforcement. Google notes in its 2018 report, 'How Google Fights Piracy':

> Since 2012, Google has terminated over 13,000 AdSense accounts and ejected more than 100,000 sites from our AdSense program for violations of our policy on copyrighted material. The vast majority of these ejections were caught by AdSense's own proactive screens. Almost all AdSense ad formats include a link that permits a copyright owner to report sites that are violating Google's policies. Copyright owners may also notify Google of violations through a webform. Each time Google receives a valid copyright removal notice for Search, we also blacklist that page from displaying any AdSense advertising in the future.[195]

More generally, the advertising industry's efforts against online piracy are undertaken on a voluntary basis. It is not a formally regulated industry in this context. Furthermore, it is not a crime in English law to make a payment to a criminal (as opposed to then handling the proceeds of a crime).[196] Other than considerations of corporate social responsibility and reputation, there is little leverage available for prompting advertising companies to go beyond what they are currently doing.

---

191. Steve Hemsley, 'Protecting Advertisers from Digital Piracy', *The Telegraph*, 14 February 2020.
192. Authors' interview with a content protection agency professional, 11 September 2020; authors' interview with a non-UK policymaker, 3 September 2020.
193. Authors' interview with a non-UK-based content protection agency, 16 June 2020.
194. *Ibid*.
195. Google, 'How Google Fights Piracy', 2018, p. 58.
196. R v GH [2015] UKSC 24, paras 20–27.

One avenue that has been used in other contexts to prevent payments to criminal groups is the imposition of targeted financial sanctions. For instance, the US imposed sanctions on EvilCorp, a Russian-based cybercriminal group involved in malware distribution in December 2019.[197] Separately, in July 2020, the EU targeted Iranian, North Korean and Russian actors involved in cyber attacks against the EU.[198] There is no current precedent for sanctions against organised crime networks involved in IP crime, and the UK only began resorting to unilateral sanctions (other than in the anti-terrorism context) in July 2020.

Designating one or more pirate groups under the UK's independent sanctions regime could serve several purposes. One would be the practical objective of preventing UK-based individuals from making payments to that group as a matter of legal obligation. It would also have the symbolic impact of affirming the UK's high-level policy commitment to IP crime and the willingness to treat organised crime networks engaged in it on a par with other serious threat actors.[199] Only relevant to the most egregious offenders, this is one potentially powerful way to target state-sponsored IP crime or pirate groups operating from non-cooperative jurisdictions.

Access Disruption

The reliance on online service providers to preclude access to illegal content is a longstanding practice. For present purposes, online service providers are understood to be broadly equivalent to the companies covered by the UK government's 'Online Harms White Paper', namely 'companies that provide services or tools that allow, enable or facilitate users to share or discover user-generated content, or interact with each other online'.[200] In particular, categories of companies relevant to this research include:

- **Internet service providers**, which enable users to access the internet.
- **Domain name registrars**, which provide domain names to users.
- **Hosting service providers**, which offer servers necessary to store data.
- **Social media**, where information about pirated content can be found.
- **Internet search operators**, which can likewise be used to find pirated content.

197. US Department of the Treasury, 'Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware', press release, 5 December 2019, <https://home.treasury.gov/news/press-releases/sm845>, accessed 9 January 2021.
198. European Council, 'EU Imposes First Ever Sanctions Against Cyber-Attacks', press release, 30 July 2020, <https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/>, accessed 9 January 2021.
199. See also Cathy Haenlein, 'Disrupting Serious and Organised Crime: What Role for UK Sanctions?', Strategic Hub for Organised Crime Research (SHOC), 18 December 2020, <https://shoc.rusi.org/informer/disrupting-serious-and-organised-crime-what-role-uk-sanctions>, accessed 10 January 2021.
200. DCMS, 'Online Harms White Paper', 15 December 2020, Question 4, <https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper#companies-in-scope-of-the-regulatory-framework>, accessed 12 January 2021.

- **Content delivery networks**, which enable swift transmission of pirate content.

Key modes of harnessing their resources to impede access to pirated content include: rights holders obtaining court injunctions; online service providers identifying pirated content; and search engines demoting search results related to pirated content.

Injunctions

Since 2003, rights holders have had the ability to apply for injunctions requiring online service providers to block access to infringing websites.[201] There appear to be no comprehensive statistics on the numbers of cases where the provision has been applied, but it is known to be used routinely.[202] In September 2020, the Premier League secured a High Court order for a new 'Super Block' on illegal streaming sites, requiring the UK's major internet service providers to conduct dynamic blocking during live events. Over 329,000 illegal live streams of Premier League football were 'blocked or disrupted' this way during the 2018–19 season.[203] However, injunctions are of limited use if directed against non-UK-based operators in countries whose courts will not enforce those injunctions.

Identification of Pirated Content

There is no general obligation on online service providers to proactively identify infringing content. Under the Electronic Commerce (EC) Directive Regulations 2002, which implement the EU's E-Commerce Directive, neither businesses that transmit information nor those that host content can be held liable as a result unless they have 'actual knowledge' of unlawful activity.[204] This is often known as a 'safe harbour provision'.

There has been discussion of further measures on the EU level. Under the Digital Services Market (DSM) Directive, which must be transposed in EU member states' domestic law by 7 June 2021,[205] a hosting provider is liable for the material its users upload unless it can demonstrate it has:

---

201. Section 97A of the Copyright, Designs and Patents Act 1988 (inserted in 2003).
202. Audrey Horton, 'IP & IT Bytes: Copyright: Website-Blocking Order Against Internet Service Providers', Bird & Bird, June 2015, <https://www.twobirds.com/en/news/articles/2015/global/ip-and-it-law-bytes-june/copyright-website-blocking-order-against-internet-service-providers>, accessed 13 November 2020.
203. Murad Ahmed, 'Premier League Steps Up War on Piracy to Protect TV Deals', *Financial Times*, 16 September 2020.
204. Regulations 17 and 19 of the Electronic Commerce (EC) Directive Regulations 2002 respectively.
205. Article 29(1) of Directive (EU) 2019/790 of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC.

> a) made best efforts to obtain an authorisation [from the rights holder], and
>
> b) made, in accordance with high industry standards of professional diligence, best efforts to ensure the unavailability of specific works and other subject matter for which the rightholders have provided the service providers with the relevant and necessary information; and in any event
>
> c) acted expeditiously, upon receiving a sufficiently substantiated notice from the rightholders, to disable access to, or to remove from their websites, the notified works or other subject matter, and made best efforts to prevent their future uploads in accordance with point (b).[206]

The UK is no longer bound by EU law and does not intend to implement the DSM Directive.[207] The EC Directive Regulations 2002, including the safe harbour provisions, therefore remain in force for now. This means that, in effect, online service operators have no obligation to proactively identify pirated content and are only required to act if they have 'actual knowledge' of such content.

Another possible change that would introduce greater obligations on online service providers but stop short of requiring them to proactively identify pirated content is the adoption of KYBC rules, which would require online service providers to record and verify the identity of their customers, as well as enable the imposition of fines for a failure to do so.[208] The rationale behind the proposal is to prevent the anonymous or pseudonymous use of online service providers, which is conducive to online IP crime and other illicit conduct. Specifically, knowing the identify of one's customer will enable online service providers to share this information with law enforcement agencies when requested.

The imposition of such requirements would effectively import one aspect of anti-money-laundering/counterterrorist-financing (AML/CTF) regulations – that is, the obligation to know one's customer – into the ecosystem of online services. This change would *not* subject online service providers to other AML/CTF-style obligations, such as the reporting of suspicious activity.

KYBC regulations can be expected to only impose a limited burden on legitimate businesses and can therefore be seen as a moderate step towards the prevention of online IP crime by

---

206. *Ibid*.
207. Chris Skidmore, 'Copyright: EU Action – Question for Department for Business, Energy and Industrial Strategy, UIN 4371, Tabled on 16 January 2020', <https://questions-statements.parliament.uk/written-questions/detail/2020-01-16/4371>, accessed 12 January 2021.
208. See Know Your Busines Customer, 'The Solution', <https://www.kybc.eu/the-solution/>, accessed 12 January 2021; BPI, 'BPI Response to the CMA Digital Markets Taskforce Call for Information', November 2020, p. 17, <https://assets.publishing.service.gov.uk/media/5fce0af6d3bf7f5d053c6bc4/Response_to_CFI_-_BPI_.pdf>, accessed 12 January 2021; Alliance for Intellectual Property, 'Alliance for Intellectual Property Response to Digital Markets Taskforce: Call for Information', August 2020, p. 3, <https://assets.publishing.service.gov.uk/media/5fce0962d3bf7f5d06b02b13/Response_to_CFI_-_AIP.pdf>, accessed 12 January 2020.

online service providers. For it to be effective, however, there has to be clarity as to which governmental agency would have the power to monitor compliance with KYBC requirements, and resources for doing so would have to be made available.

Search Engine Demotion

By comparison to other online service providers, search engines have the opportunity to reduce the visibility of pirated content as opposed to removing it, which they cannot do. In 2014, then Culture Secretary Sajid Javid and Business Secretary Vince Cable wrote to Google, Microsoft and Yahoo asking them to prevent search results from directing users to infringing websites.[209] Search engines' policies prohibit advertising products that infringe copyright.[210] However, there have been instances in the past where illegal websites were able to place paid advertisements on Google.[211]

In addition to refusing to place advertisements of such products, major search engines have now committed to demoting copyright-infringing websites in UK users' search results.[212] In 2017, representatives of Google, Bing and Yahoo adopted a voluntary Code of Practice on Search and Copyright following discussions with representatives of UK creative industries. This follows Google's unilateral efforts to downgrade websites in search results based on the number of Digital Millennium Copyright Act complaints they attract.[213]

Payment Disruption

In order to enable customers to pay for pirated content in a convenient and seemingly legitimate manner, website operators need to be able to accept payments. For bank cards, this involves access to an acquiring bank (acquirer) or a payment service provider, which rely on card payment schemes such as Visa or Mastercard to make the payment. As discussed above, in some cases, payments in crypto-assets such as Bitcoin may be involved.

---

209. Matthew Wilson, 'UK Government Warns Search Engines Over Piracy', Kitguru, 4 September 2014, <https://www.kitguru.net/channel/generaltech/matthew-wilson/uk-government-warns-search-engines-over-piracy/>, accessed 13 November 2020.
210. Amy Gesenhues, 'You Can't Advertise That: The Big List of Prohibited Ads Across Social and Search Platforms', SearchEngineLand, 17 September 2019, <https://searchengineland.com/you-cant-advertise-that-the-big-list-of-prohibited-ads-across-social-and-search-platforms-322222>, accessed 13 November 2020.
211. @briankrebs, 'It's nice that my site comes up tops in Google on the term "booter" and almost top for "stresser." What would be nicer is if @Google didn't accept ad money from DDoS-for-hire services, full stop. BTW, this is not a new thing', Twitter, 13 May 2020, <https://twitter.com/briankrebs/status/1260396524137218048>, accessed 4 February 2021.
212. This commitment has been helpful. Authors' interview with an in-house content protection agency, 20 July 2020.
213. Google, 'How Google Fights Piracy'.

Acquiring Banks

The acquiring bank's function is to offer a merchant account, which is used by the website operator to receive customers' payments. It is distinct from the website operator's other bank accounts and may or may not be held in the same bank. For a card payment to be possible, the acquiring bank and the bank that issues the payer's card (that is, the debit or credit card that belongs to the website's user) must be members of the same card payment scheme.

To obtain the ability to accept card payments, the website operator therefore has to approach an acquiring bank, which is subject to AML obligations that include conducting customer due diligence (CDD) and filing suspicious activity reports (SARs). Alternatively, the website operator may turn to a payment service provider that will process customers' card payments. In that case, the payment service provider will in effect place its own merchant account with an acquiring bank at the website operator's disposal. The acquiring bank will not be able to disaggregate the website operator's transactions from those of the payment service provider's many other customers. Nor will it do CDD on the website operators. This is the responsibility of the payment service provider, which is a regulated financial institution in its own right.

For legitimate businesses, the use of a certain acquiring bank or payment service provider is a function of considerations such as cost and convenience. By contrast, organised crime networks engaged in online piracy seek to obtain payment capabilities which they, by virtue of regulatory obligations on banks and payment service providers, are not allowed to have. Their behaviour therefore falls on the spectrum between deceiving banks and payment service providers or colluding with them.

Central to this is a concept that is often called 'transaction laundering', which refers to the misrepresentation of the nature of one's business to obtain a merchant account. A merchant account is highly advantageous, as the flow of income expected in such an account is much higher than a personal one. Transaction activity that looks suspicious in a personal account – such as an influx of multiple small payments – is less likely to arouse suspicion in a merchant account. For instance, a person engaged in the provision of pirated content could claim to be selling craft soap and set up a website that purports to show that. This website would be presented to the acquiring bank as evidence of that person's business activities. In truth, however, all of that person's customers would come to the payment portal through a wholly different website where pirated content is offered and which constitutes the merchant's true business.[214]

Transaction laundering can be detected through a combination of open source analysis of customers and test purchases.[215] For instance, it may be possible to establish that: traffic volumes on the 'legitimate website' do not match the rate of payments processed; the merchant's account activity is inconsistent with that of a business that manufactures craft soap; and no soap can in fact be bought through the website in question.

214. Authors' interview with a content protection agency official specialised in finance, 3 March 2020.
215. *Ibid*.

Often, however, acquiring banks have little incentive to undertake such investigations. They earn fees from transactions they facilitate and thus have a financial interest in their customers' success.[216] Furthermore, regulatory focus on transaction laundering in the UK and the EU has been limited to date.[217] There is little to no guidance as to how much is expected of acquiring banks to ensure they do not offer merchant accounts to criminals. Nor has there been concerted engagement by rights holder groups with financial regulators in various countries to draw their attention to this matter, despite its key role in facilitating the commission of multiple crimes.[218]

One limitation of such engagement is that many pirate website operators are based in less or non-cooperative jurisdictions, including China,[219] Southeast Asia[220] and Africa,[221] where their access to merchant accounts is unimpeded. A strong regulatory effort across the UK and the EU could result in further displacement. However, the inconvenience and cost this would entail for organised crime networks, as well as the symbolic importance of driving such businesses out of the UK's and other European countries' financial systems, would make this effort worthwhile. This report therefore recommends leveraging the UK government's Special Operations Community Network (SOCNet), which has liaison officers stationed in key countries of interest.[222]

Payment Service Providers

The same comments apply to payment service providers. They fulfil the same role of enabling access to the global payments infrastructure and financial system. Large and well-known payment service providers tend to be highly effective in answering ad hoc law enforcement agencies and rights holders. Despite the evidence above highlighting PayPal as the payment processor of choice for pirate sites, they were consistently mentioned as displaying best practice against piracy,[223] with the exception of an investigator who had reservations about PayPal's approach to unfreezing accounts unless conclusive evidence of wrongdoing could be provided.[224]

---

216. Authors' interview with a content protection agency official specialised in finance, 3 March 2020; US Department of Homeland Security, 'Combating Trafficking in Counterfeit and Pirated Goods', p. 7.
217. Authors' interview with a content protection agency official specialised in finance, 3 March 2020.
218. Authors' interview with a content protection agency professional, 11 August 2020.
219. Authors' interview with a former UK law enforcement investigator, 24 February 2020; authors' interview with a content protection agency official specialised in finance, 3 March 2020.
220. Authors' interview with a content protection agency professional, 11 September 2020.
221. Authors' interview with a content protection agency professional, 17 July 2020. See also European Commission, 'Counterfeit and Piracy Watch List'.
222. HM Government, *Serious and Organised Crime Strategy*, Cm 9718 (London: The Stationery Office, 2018), p. 58.
223. Authors' interview with two senior UK law enforcement officers, 13 August 2020; authors' interview with an ISP, 20 July 2020; authors' interview with a content protection agency professional, 11 July 2020.
224. Authors' interview with an in-house content protection person, 20 July 2020.

On the other hand, since it is typically easier to set up a payment service provider than a bank, there have long been concerns that some providers may enter the industry with the intention to service higher-risk customers in return for higher commission fees.[225] There is evidence of this happening in the US, where a series of enforcement actions disclosed collusion between online gambling operators and their payment service providers.[226] As with acquiring banks, to what extent this is happening in the context of online piracy is a matter ripe for dialogue between rights holders and financial regulators.

A starting point could be rights holder groups sharing among themselves the information on countries where they believe[227] acquiring banks and payment service providers that process piracy-related payments are based. This information could form the basis for a dialogue with financial regulators in respective jurisdictions. Its ultimate objective would be for regulators to clarify and enforce expectations in relation to detecting transaction laundering, which would in due course diminish organised crime networks' ability to access payment facilities.[228]

Card Payment Schemes

Card payment schemes are another key player in the payment ecosystem with the ability to disrupt the subscription fee-based business model. Their function is to enable payments between member banks, specifically from the bank that issued the payer's debit or credit card to the recipient's acquiring bank. Participating banks abide by the respective scheme's rules, which include, among other things, compliance with AML/CTF requirements.

A key measure of fraudulent activity used by payment schemes is the chargeback rate on individual accounts. If a customer believes they have not received the product or service they paid for, they can initiate a chargeback dispute via their issuing bank. The issuing bank will request the payment to be reversed and the money to be provisionally returned from the merchant's acquiring bank. This is a major selling point for many payment scheme providers. The issuing bank will then review the customer's claim and decide if the chargeback is justified. If the issuing bank and acquiring bank disagree over the chargeback, they can refer the dispute to arbitration by the payment scheme.[229]

Payment schemes penalise acquiring banks for high chargeback rates, which incentivises acquiring banks to avoid businesses that frequently face chargebacks.[230] In extreme examples, acquiring banks may be excluded from the payment scheme due to excessive chargeback rates.

---

225. Authors' interview with a rights holder, 19 March 2020.
226. Leonard L Gordon, 'Hanging Out to Dry: FTC's Ongoing Pursuit of Credit Card Laundering Has Reached an Apex', *Lexology*, 14 December 2018.
227. For instance, based on test purchases they conduct.
228. Authors' interview with a non-UK content protection agency professional, 16 June 2020.
229. Signifyd, 'Chargeback Process: An In-Depth Look', <https://www.signifyd.com/resources/fraud-101/chargeback-process-in-depth/>, accessed 4 February 2021.
230. Authors' interview with a former foreign law enforcement representative, 24 February 2020.

Project Chargeback, which is run by Canada's Royal Canadian Mounted Police, aims to promote awareness of the chargeback process among customers who have mistakenly bought counterfeit goods.[231] Doing so affects the ease with which sellers can access the financial system. However, this approach only works for cases where the customer is unhappy with the goods or services provided and is ineffectual for consensual transactions where both parties obtain what they want. This is not always the case for piracy, as many consumers knowingly purchase illegal ISDs, services or subscriptions.

The payment schemes' ability to do more in policing payments related to online piracy is constrained by the lack of a direct relationship with payment senders and recipients, which is intermediated by issuing and acquiring banks respectively.[232] Pieces of transactional information available to payment schemes include the four-digit merchant category code (MCC), which identifies the merchant's main line of business, and billing descriptor, the short payment description that becomes available on the customer's bank statement.[233] A number of businesses served by a single acquiring bank will have the same MCC. In contrast, the billing descriptor may enable the payment scheme to identify the merchant involved in the payment, but a single merchant may have several billing descriptors and so the transactional picture will be incomplete. Nor will the payment scheme have access to CDD information, which is vital for understanding the merchant's business.

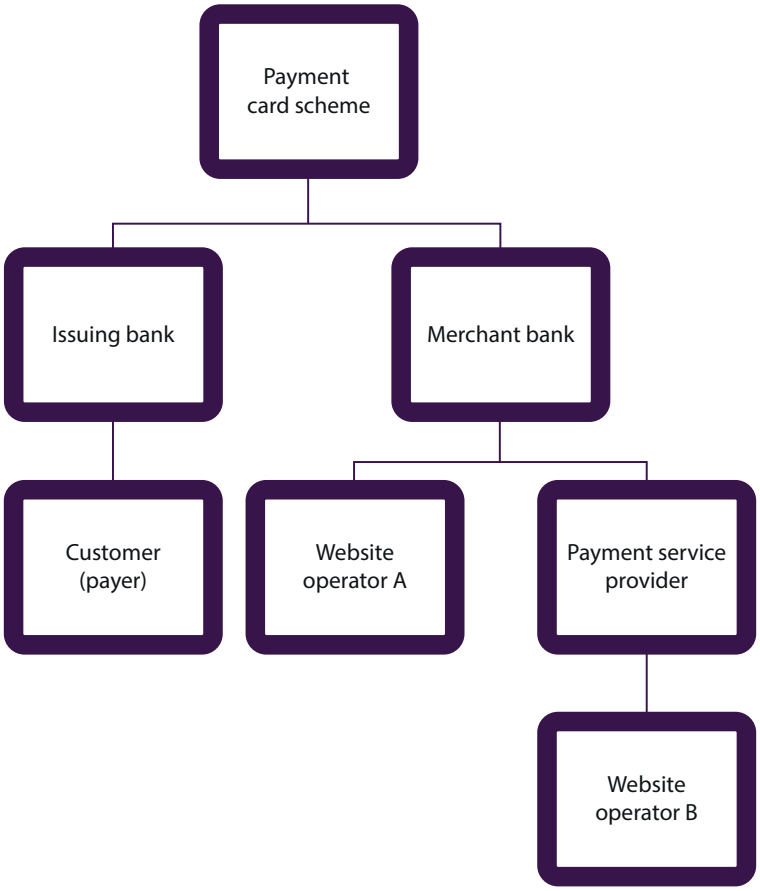
Both Visa and Mastercard – two major international card payment schemes – have anti-piracy policies in place.[234] Notwithstanding the general policy of relying on acquirers, in some cases payment schemes conduct manual checks of merchants' websites and do test purchases to identify illicit behaviour. Furthermore, both Visa and Mastercard have fraud and excessive chargeback policies, which require acquiring banks to report on merchants that exceed a prescribed chargeback threshold and work with such merchants to resolve the problem. Finally, Visa and Mastercard respond to specific ad hoc complaints from rights holders.

Nonetheless, much more can be done. Payment card schemes have at their disposal the powerful weapon of disconnecting a participating bank if it is found to be a conduit for illicit payments, but they only have limited ability to identify cases that merit investigation. Information that would enable them to focus attention on high-risk areas could be of value. This could be achieved by extending rights holders' engagement with regulators, as discussed above, to encompass

231. Authors' interview with a Canadian law enforcement officer, 6 July 2020. See also Catherine Saez, 'Canada's Anti-Counterfeiting Chargeback Project: Paying Back Deceived Consumers', Intellectual Property Watch, 12 September 2016, <https://www.ip-watch.org/2016/09/12/canadas-anti-counterfeiting-chargeback-project-paying-back-deceived-consumers/>, accessed 4 February 2021.
232. Authors' interview with a content protection agency official specialised in finance, 3 March 2020; authors' interview with a former UK law enforcement investigator, 19 March 2020.
233. See Mastercard, 'Excessive Chargeback Programme', 2018, <https://globalrisk.mastercard.com/wp-content/uploads/2018/07/Mastercard_ECP_Module.mp4>, accessed 4 February 2021.
234. See Mark MacCarthy, 'What Payment Intermediaries Are Doing About Online Liability and Why It Matters', *Berkeley Technology Law Journal* (Vol. 25, No. 2, Spring 2010), pp. 1037–120.

card payment schemes. Such tripartite dialogue could aim to develop a common understanding of high-risk geographies in the context of online piracy and of the efforts that card payment schemes can reasonably take to cut off OCGs involved in this crime. A secondary benefit of such engagement for the payment schemes would be to promote an up-to-date understanding of what they can and cannot do, which can be complex for law enforcement, policy officials and rights holders to grasp.

Figure 7: Key Figures in Processing Card Payments



Source: Author generated.

Crypto-Asset Service Providers

Crypto-asset service providers, such as crypto exchanges, are likely to have a significant role to play in preventing online piracy in the future. For now, the share of crypto-asset payments in the piracy economy remains marginal but growing.[235] This is likely a reflection of the relative

235. According to Industry Trust data, five percent of people surveyed who paid for infringing content did so in crypto-assets. See Industry Trust, 'Moments Worth Paying For Consumer Research', March 2020.

complexity for the average user of paying in crypto-assets. The need to pay in crypto-assets may also alarm those users who believe they are buying for a legitimate service. Meanwhile, their decentralisation makes them an imperfect store of value for criminals.

The potential use of crypto-assets in the future as a means to bypass the traditional financial sector has consistently been highlighted as a risk.[236] In some cases, it can help avoid reliance on AML/CTF-regulated businesses altogether because a transfer of crypto-assets, such as Bitcoin, does not require the creation of an account with any crypto-assets service provider. In practice, however, most users are likely to use a crypto-asset service provider if they wish to transact in crypto-assets.[237]

Since January 2020, crypto-asset service providers are subject to AML/CTF regulations in both the UK and the EU.[238] This means that crypto-asset service providers have to do CDD and file SARs in much the same way as banks, and they too will need to make sure they do not onboard customers who are engaged in providing pirated content. The ability to do so is bolstered by blockchain analytics, namely the ability to analyse publicly available transaction data recorded on the respective virtual asset's blockchain. Among other things, blockchain analytics can help crypto-asset service providers warn users against or even prevent them from making payments to known suppliers of pirated content. To ensure that blockchain analytics companies include infringing websites in their coverage, it is necessary that there be demand for this among crypto-asset service providers. Engagement with these providers by the regulator is therefore crucial, as much like their traditional counterparts, they are likely to be unfamiliar with the dynamics of IP crime.

Strengthening Financial Investigation

The UK's 2016–20 IP enforcement strategy championed greater use of financial investigations and the Proceeds of Crime Act in piracy cases, a commitment maintained in the forthcoming strategy.[239] There are at least six dedicated financial investigators and a further six financial intelligence officers working across the IPO Intelligence Hub and PIPCU. These human resources represent a clear commitment to a 'follow the money' strategy, with at least £1.2 million secured through asset confiscation in IP crime cases in recent years.[240]

236. Authors' interview with an ISP, 4 August 2020; authors' interview with a content protection agency professional, 11 August 2020; authors' interview with in-house legal counsel at a rights holder, 8 July 2020.
237. TokenInsight, '2019 Q1 Cryptocurrency Exchange Industry Research Report', April 2019, p. 18, <https://tokenin.cn/api/upload/dashboardPdf/TI-Cryptocurrency%20Exchange%202019Q1-Final.pdf>, accessed 3 February 2021.
238. See Section 3 of the Money Laundering and Terrorist Financing (Amendment) Regulations 2019 (in the UK) and Article 1(1)(c) of Directive 2018/843 of 30 May 2018 Amending Directive (EU) 2015/849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, and Amending Directives 2009/138/EC and 2013/36/EU (in the EU).
239. IPO, 'Protecting Creativity, Supporting Innovation', pp. 21–22.
240. IPO, 'IP Crime and Enforcement Report 2018–2019', pp. 4–6.

It is nonetheless difficult to track the extent to which convictions for financial offences and routine asset confiscation have increased as a result of the IP enforcement strategy. Many IP crime cases are tried under the Fraud Act 2006, not the Copyright, Designs and Patents Act 1988, which complicates the collection of statistics about outcomes in IP crime cases.[241] However, it appears that the use of financial intelligence is becoming increasingly mainstream in UK piracy investigations, though interviewees noted far more could be done to share intelligence and typologies with the financial sector.[242] In turn, this should create incentives to open parallel money-laundering investigations since certain investigatory measures require such an investigation to be open and ancillary charges for financial offences can be far more punitive than weaker penalties for IP crime.[243]

Existing Challenges

Access to sensitive financial information, such as bank transaction records, is an inevitable challenge in investigating any crime. This information is subject to legal safeguards, including the need to obtain court orders, that hamper the speed of the investigation or require specialist permission to apply for.[244] One particular challenge is the inability to draw on evidence from financial investigations in private prosecutions, which account for a significant number of IP crime cases tried in the UK. A 2020 UK government inquiry into safeguarding private prosecutions received submissions suggesting that they 'are particularly important for intellectual property crime, because the private sector is able to supply the necessary specialist expertise and resources that the CPS and the police cannot'.[245] Yet, although substantial sentences and confiscation orders can be issued in these cases,[246] only limited financial evidence can be collected and used in the course of preparing and prosecuting a private case as private actors cannot conduct financial investigations.[247]

241. Martin Brassell and Ian Goodyer, *Penalty Fair? Study of Criminal Sanctions for Copyright Infringement Available Under the CDPA 1988* (London: Intellectual Property Office, 2015), p. 4.
242. Authors' interview with UK law enforcement investigator A, 12 August 2020; authors' interview with UK law enforcement investigator B, 12 August 2020; authors' interview with a UK law enforcement investigator, 10 August 2020; authors' interview with a UK law enforcement investigator, 24 July 2020.
243. Authors' interview with UK law enforcement investigator A, 12 August 2020.
244. Authors' interview with a non-UK law enforcement policy official, 31 August 2020.
245. House of Commons Justice Committee, 'Private Prosecutions/Safeguards, Ninth Report of Session 2019–21 Report'.
246. UK Parliament, 'Response to Request for Evidence from the Justice Select Committee Concerning Safeguards Against Prosecutorial Abuse in Victim-Led Private Prosecutions: Written Evidence from Fact, Sky Uk Limited, The Football Association Premier League Limited (Pps0016), Ari Alibhai And Qeb Hollis Whiteman Chambers', <https://committees.parliament.uk/writtenevidence/8269/html>, accessed 7 February 2021.
247. Authors' interview with UK law enforcement investigator C, 2 February 2021.

Furthermore, although the UK has seen more financial investigation resources dedicated to IP crime in recent years, PIPCU's capacity is overstretched and tasking in local police forces is unpredictable.[248] This results in several deficiencies that are compounded by the:

- **Lack of reliable information on the overall money made through online piracy**.[249] This is partly a consequence of the fact that proceeds are likely to be accumulated in overseas jurisdictions.[250] There is currently no standard formula for estimating criminal gain – or damages – from piracy.
- **Dearth of understanding as to how much criminals make at various stages of the IP piracy supply chain**.[251] Among other things, this can detract from the ability to accurately portray the gravity of the offence in court.[252]
- **Limited asset confiscation[253] and damage recovery**,[254] which reflects the fact that criminals are adept at dissipating their assets before the legal process concludes and a lack of capacity to follow financial leads at the outset of an investigation.[255]
- **Length of time taken to carry a Proceeds of Crime Act confiscation case through to a successful conclusion**. This is due to the procedures put in place by the courts to ensure diligence on behalf of investigators and fairness to respondents, combined with limited resources, among other factors. Financial investigations can therefore be time consuming and expensive.

Opportunities for Improvement

The effectiveness of financial investigation largely depends on the quality of financial information available to law enforcement agencies and their capacity to analyse it.[256]

Research for this report confirms that private sector efforts are underway to improve the situation, but much remains to be done. For instance, FACT is engaged in collecting financial information with a view to attributing infringing content and websites to specific individuals and/or groups.[257] This analysis is supported by efforts undertaken by individual members, such as accessing domain registration data, conducting social media research and undertaking test

248. Authors' interview with UK law enforcement investigator A, 12 August 2020.
249. Authors' interview with a UK policymaker, 21 July 2020.
250. Authors' interview with a former UK law enforcement investigator, 24 February 2020; authors' interview with a German-based AML/CTF consultant, 3 March 2020; authors' interview with a content protection agency professional, 15 July 2020.
251. Authors' interview with a UK policymaker, 21 July 2020.
252. Authors' interview with a non-UK policymaker, 3 September 2020.
253. Authors' interview with UK law enforcement investigator B, 12 August 2020.
254. Authors' interview with a content protection agency professional, 15 July 2020.
255. Authors' interview with in-house legal counsel at a rights holder, 8 July 2020.
256. Authors' interview with an e-commerce intermediary, 24 September 2020; authors' interview with a UK policymaker, 21 July 2020.
257. Authors' interview with in-house legal counsel at a rights holder, 8 July 2020.

purchases.[258] The information collected in this manner is provided to law enforcement on a case-by-case basis.[259]

Further opportunities to strengthen financial investigation by bolstering information sharing should also be explored. This should include a public–private intelligence sharing partnership operated and maintained by the IPO Hub or PIPCU.[260] Other law enforcement agencies would also benefit from having access to information and expertise held within the IPO.[261] Key categories of potential participants in expanded information sharing are law enforcement agencies (including cybercrime units), financial institutions, online service providers, rights holders and advertising networks. High-level governmental support will be crucial for private sector involvement.[262] Here, the UK can learn from the US Intellectual Property Rights Center, who recently concluded the trial of a pilot E-Commerce Working Group that brought together e-platforms, shipping lines and payment companies.[263] This serves as one example of intersectoral partnership and leadership of the kind the UK could benefit from.

Finally, another gap in financial responses to online piracy is the scant effort made to ensure that banks do not process customers' payments for infringing content. As discussed above, the primary objective of lists such as PIPCU's IWL and WIPO Alert is to ensure that advertising networks do not do business with infringing websites. These are untapped sources of highly useful financial information. Information linked to those websites should be obtained from test purchases, analysed and disseminated across financial institutions.[264]

This approach is similar to infringing website monitoring that is already done by some private sector companies, but whereas those companies' main audience tends to be rights holders,[265] it would be tailored to the financial industry. It could undermine those OCGs that rely on user fees, but the powerful effect that this sort of blacklisting can have on businesses necessitates near-complete accuracy and availability of procedural safeguards, similar to the approach currently taken by PIPCU. Moreover, there will be an inevitable displacement effect to other services. Financial disruption must therefore be accompanied by concerted enforcement responses that target the most egregious offenders.

---

258. *Ibid*.
259. Authors' interview with legal counsel for a rights holder, 8 July 2020.
260. Authors' interview with a former UK law enforcement investigator, 19 March 2020; authors' interview with a payment company representative, 14 August 2020.
261. Authors' interview with UK law enforcement investigator B, 12 August 2020.
262. Authors' interview with in-house content protection at a rights holder, 20 July 2020.
263. Authors' interview with US law enforcement, 24 August 2020; US Department of Homeland Security, 'Combating Trafficking in Counterfeit and Pirated Goods', p. 31.
264. Authors' interview with a content protection agency professional, 11 August 2020; authors' interview with a payment intermediary, 14 August 2020.
265. Authors' interview with a content protection agency professional, 14 July 2020; authors' interview with a content protection agency professional, 11 September 2020.

Demand Reduction: Consumer Education

While this chapter has focused primarily on supply-side solutions in the piracy financial chain, there certainly is a place for demand reduction through consumer education in undermining subscription-based models. Some consumers find it hard to identify the difference between legitimate and illegitimate sources, an issue that the presence of advertising and legitimate payment providers compounds. The availability of well-known payment methods legitimises sites run by those selling counterfeit and pirated goods online.[266] The 2019 OCI Tracker found that 62% of internet users claimed to be 'confident' in their ability to identify legal from illegal content online, and the OCI Tracker 9th Wave in 2020 noted that 'ambiguity around regulation' meant there was 'uncertainty' regarding whether some sources were technically legal or not.[267] Interventions, such as Find Any Film and Get it Right From a Genuine Site, have been introduced to guide consumers to legitimate sources (more below), with the latter concluding that three in 10 are confused as to the legality of the content online, with the youngest cohorts most likely to fall under this bracket.[268] By comparison, the extent to which consumers who pay for infringing services are unwitting about their legitimacy is unclear. One 2019 study of all 28 EU member states suggests that self-reported awareness of legal services reduced illicit consumption of film but not TV, with no statistically significant impact on music consumption.[269]

In 2020, the IPO released analysis suggesting consumers were most influenced by awareness-raising campaigns showing that IP piracy and counterfeiting fund organised crime and terrorism.[270] The 'believability' of such messages is heavily influenced by the source of the evidence, with some sources not considered to be credible and some messages felt to be mere 'scare tactics'.[271] Simple and eye-catching messages were considered the best medium of delivery, with emotional

266. Official data provided by PIPCU; authors' interview with a law enforcement agency, 10 August 2020; Incopro, 'The Revenue Sources for Websites Making Available Copyright Content Without Consent in the EU', p. 19; US Department of Homeland Security, 'Combating Trafficking in Counterfeit and Pirated Goods', p. 7.
267. IPO*, Online Copyright Infringement (OCI) Tracker*, 9th Wave; IPO*, Online Copyright Infringement Tracker Latest Wave of Research (March 2018): Overview and Key Findings* (London: The Stationery Office, 2018).
268. Official data supplied by the IPO; Find Any Film, <https://www.findanyfilm.com/>, accessed 4 February 2021; IPO, 'Get It Right from a Genuine Site Copyright Campaign Update', 19 January 2017, <https://www.gov.uk/government/news/get-it-right-from-a-genuine-site-copyright-campaign-update>, accessed 4 February 2021.
269. EUIPO, *Online Copyright Infringement in the European Union: Music, Films and TV (2017–2018), Trends and Drivers* (Alicante: EUIPO, 2019), p. 7, <https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/quantification-of-ipr-infringement/online-copyright-infringement-in-eu/online_copyright_infringement_in_eu_en.pdf>, accessed 4 February 2021.
270. EUIPO, 'IP Youth Scoreboard', 2015.
271. IPO*, Online Copyright Infringement (OCI) Tracker*, 9th Wave.

messages more powerful than factual ones.[272] This suggests that credible research on the connections between IP crime and negative personal or societal outcomes can be used in education campaigns.[273]

Results from both the 2016 and 2019 EUIPO Youth Scoreboard sample suggests the threat of a negative impact on personal safety and risk are the most influential factors in the decision not to pirate copyright infringing works or buy counterfeit goods. In 2019, the EUIPO's IP Youth Scoreboard showed that 51% of 15–24 year olds consider safety an important factor when accessing online content.[274] Up to 81% claim they would think twice if they were aware that their device could be infected with malware.[275] This rises to 83% if they were aware their credit card details could be stolen.[276] This youth sample is significant, as young people often represent the largest proportion of infringers in the UK and abroad.[277]

Table 3: 15–24-Year-Old Consumer Message Testing

	Your credit card details could be stolen		**You risk your computer becoming infected by viruses or malware**		**You can risk a fine or another sanction**		**Money spent on fake products goes to organised crime**	
	2016	2019	2016	2019	2016	2019	2016	2019
EU average	84%	83%	78%	81%	75%	75%	72%	66%
UK average	87%	86%	81%	86%	75%	79%	73%	69%

Source: Adapted from EUIPO, 'IP Youth Scoreboard', 2019.

The results of a joint campaign between Crimestoppers and the Industry Trust corroborate that evidence of personal risk resonating well with audiences.[278] The intervention targeted

272. *Ibid*.
273. Organisations such as the Industry Trust conduct quarterly, yearly and ad hoc trackers that provide this type of evidence base. The IPO's Online Copyright Tracker could be adapted in the future to measure the incidence of negative personal, financial, emotional and physical outcomes as a result of infringement activity.
274. EUIPO, 'Intellectual Property and Youth Scoreboard', 2019, p. 64.
275. *Ibid*.
276. IPO*, Online Copyright Infringement (OCI) Tracker*, 9th Wave; EUIPO, 'Intellectual Property and Youth Scoreboard', 2019.
277. IPO*, Online Copyright Infringement (OCI) Tracker*, 9th Wave. Infringement generally decreases in the sample by age, though it should be noted there is a slight increase again among the 55+ age group for music, film and live sport infringement.
278. IPO, 'IP Crime and Enforcement Report 2019-20', p. 72.

consumers searching for pirated content and delivered advertising banners with messages laying out the illegality, online safety and technology risks to consumers. The campaign has generated 18 million impressions, with a post-campaign survey suggesting those exposed to the messaging were two-and-a-half times more likely to search for legal streaming services.[279] The 2018 Online Copyright Tracker saw 'I fear they may have viruses/malware/spyware' listed for the first time among the top five reasons why consumers used legal paid services.[280]

Several experts further stressed the need to educate legislators and enforcement agencies of the dangers of piracy. Compared to the general public, policymakers may be far more likely to be receptive to the financial impact of the situation, including lost jobs, income and taxation.[281]

Figure 8: Example of Crimestoppers Campaign

Source: Crimestoppers campaign artwork, provided by the Industry Trust.

279. *Ibid*.
280. IPO*, Online Copyright Infringement Tracker Latest Wave of Research (March 2018)*, Slide 29. All sampled aged 12+ who have paid to download or stream/access any of the six content types in a three-month period.
281. Authors' interview with a content protection industry representative, 17 July 2020.

Conclusion and Recommendations

THIS REPORT ARGUES that financial disruption must be at the heart of government policy and industry initiatives to combat AV piracy. It outlines how organised crime networks exploit vulnerabilities in the formal financial sector to facilitate payments from consumers and advertisers, and how recent trends in the world of IPTV have brought to light the ubiquity of paying pirates directly to access illegal content, in the same way consumers would usually pay for legitimate goods and services.

There is great promise in the UK and the European Commission's championing of a 'follow the money' response to IP crime, but current efforts have not greatly reduced opportunities to generate significant criminal profit from piracy. In sum, the potential of financial intelligence and investigations remains greatly underused. Changing this requires action on the demand side of the problem, by making consumers more aware of the risks they face as a consequence of purchasing pirated content, and a more concerted approach to the supply-side factors which enable consumers' access to that content and criminals' ability to receive payments for it.

Tangible victories can be won by disrupting the options that pirate criminals have to distribute and monetise IP-infringing content. For that to happen, a wide range of stakeholders need to come together and commit to action against piracy. In this vein, this report recommends the IPO, PIPCU or another competent authority should establish a public–private partnership that brings together government, law enforcement, financial institutions, online service providers, rights holders and advertising networks to share intelligence and typologies about piracy.[282]

This cross-sector coordination must be met with greater coordination within the public sector and law enforcement. This report finds there is still considerable fragmentation in how piracy is investigated in the UK. The negative impact of a lack of a centralised reporting system for IP crime is clear and a review of how effectively IP crime-related intelligence is collected and shared across law enforcement is needed. IP crime requires a whole-of-system approach that unites government agencies and draws on investigative skills across the UK SOC policing network. This report does not promote a specific solution, but notes that some stakeholders suggested the IPO Intelligence Hub could play a greater role in coordinating action across law enforcement and government agencies to address IP crime.[283] This includes intelligence sharing across law enforcement partners such as PIPCU, Trading Standards, local police forces and the 10 ROCUs across England and Wales to ensure that specialist capabilities in areas like cybercrime, financial investigation and fraud are available to pursue IP crime cases. Significant benefits could come

282. See Nick J Maxell and David Artingstall, 'The Role of Financial Information-Sharing Partnerships in the Disruption of Crime', *RUSI Occasional Papers* (October 2017).
283. Feedback received in IP and law enforcement validation workshop, 18 January 2021.

from integrating IP crime as a priority into the UK's new SOC tasking system, which will deliver a single, systematic and agreed approach to tasking across this system.[284]

Where financial investigations lead to money-laundering prosecutions or asset confiscations, their impact should be recorded and disseminated to encourage further resource allocation and uptake of those methods. Showing the private sector that their contributions are leading to visible, positive results – and offering public recognition of this where possible – is the best way of encouraging them to report valuable intelligence at scale rather than on a case-by-case, ad hoc basis. This action should be married with more targeted local action where 'follow the money' approaches are seen as integral to preventing criminals acting with impunity in the UK. In the meantime, PIPCU and the IPO Intelligence Hub should continue to accept intelligence from the private sector and communicate how financial intelligence from test purchases and private investigations should be gathered and transferred.

For industry, and financial intermediaries in particular, there is a vital need to evaluate how exposed they are to criminal profits derived from IP crime. There is limited awareness of this crime type and an overdue responsibility to understand, as accurately as possible, how much of this activity they are facilitating and begin realigning their internal priorities and compliance processes to respond to that. This could be supported by information sharing within the public–private partnership referenced above. At a minimum, financial institutions commonly abused by pirates should have clear points of contact who are dedicated to dealing with this specific issue. One thing which may help in achieving this is to stress that financial institutions are themselves having their own IP infringed for the purpose of making pirate services look more legitimate. The problem is a lot closer to home than many currently think.

Finally, at the higher, diplomatic level, IP-related crimes should no longer be on the margins of the UK's interaction with foreign jurisdictions. This should involve greater engagement with financial regulators abroad to ensure that the right level of regulatory scrutiny is being applied to acquiring banks that may be wittingly or unwittingly processing payments for infringing content. The imposition of targeted financial sanctions by the UK against one or more organised crime networks involved in piracy could serve as a symbolic acknowledgement of the threat posed by IP crime and a sign of political commitment to tackling it. Further, piracy is a transnational crime that will rely on the ability to work with law enforcement abroad following the UK's exit from the EU.

There is a long way to go to take the profit out of piracy. This report aims to lay out a blueprint for changing that by detailing what can be achieved when financial investigation approaches are embraced by a wide coalition of stakeholders, all united by the common goal of enforcing the law against criminals who wilfully disregard it.

284. NCA, 'Leading the UK's Fight to Cut Serious and Organised Crime'.

Recommendations

The recommendations below are addressed to UK audiences. However, almost all of them are internationally applicable. This is particularly true of recommendations for the private sector, including rights holders, the financial sector and online service providers working across multiple geographies.

All Stakeholders

1. IP crime requires a whole-of-system approach that coordinates agencies across government and activates investigative skills across the UK SOC policing network. This includes the IPO Intelligence Hub, PIPCU, Trading Standards, local police forces and the 10 ROCUs across England and Wales to ensure that specialist capabilities in areas like cybercrime, financial investigation and fraud are mobilised to pursue IP crime cases.
2. The IPO or PIPCU should establish a public–private partnership to share intelligence across law enforcement agencies, financial institutions, online service providers and advertising networks. Financial institutions, advertising intermediaries and rights holders should be proactive in volunteering their participation.
3. Closer public–private collaboration and sustained financial support for consumer education campaigns is needed to ensure they are evidence-based and tested among the target audience for maximum effectiveness.

Public Sector and Law Enforcement

4. In the context of the UK's review of online harms, KYBC rules should be introduced to require online service providers to record and verify, to the extent possible, the identity of their business customers. Resources should be made available for monitoring and enforcing compliance with these rules.
5. The financial investigation capacity and resourcing of PIPCU, the IPO Intelligence Hub and Trading Standards should be maintained and increased as necessary to ensure they are able to conduct effective financial intelligence gathering and investigations.
6. Strategic assessments of IP crime should draw on sources of financial intelligence such as SARs and parallel financial investigations. Typologies should be developed and disseminated to financial institutions and other private sector stakeholders via appropriate industry groups such as UK Finance and the Joint Money Laundering Steering Group.
7. The IPO and PIPCU should work together with the Foreign, Commonwealth and Development Office for the latter to consider the possibility of imposing targeted financial sanctions on OCGs involved in the distribution of IP-infringing content from non-cooperative jurisdictions.
8. Information should be compiled on jurisdictions whose financial services are most often used to receive payments for IP-infringing content. This should inform engagement with foreign financial regulators and encourage them to incentivise regulatory scrutiny of acquiring banks.

9. The FCA should conduct a thematic review of the ability of acquiring banks to detect customers who are engaged in selling illicit services, including the provision of IP-infringing content.
10. The FCA should educate crypto-asset service providers about the risks of facilitating payments for IP-infringing content. This is to ensure that these risks are emphasised alongside other, more familiar forms of crypto-asset-related crime.
11. The Alliance for IP, WRi Group (a brand protection company) and IPO should incorporate financial investigation and analysis modules in their training courses, to ensure opportunities for confiscation or ancillary charges are always considered in IP crime cases.
12. Collaboration with the UK government's Special Operations Community Network (SOCNet) team could be enhanced to better target the infrastructure and financial aspects of IP crime, including liaison officers stationed in Hong Kong, the US and Southeast Asia.

Private Industry

13. Financial institutions should evaluate their exposure to the proceeds of IP crime and commit to measures to improve prevention, detection and reporting.
14. Financial institutions should seek access to WIPO Alert, the European Commission's Counterfeit and Piracy Watchlist (open access) and PIPCU's Infringing Website List. These lists should be regularly analysed to identify their exposure to piracy and take appropriate action, such as terminating their relationship with pirate services and/or filing a SAR.
15. Regardless of the formal introduction of KYBC rules, online service providers should record and verify, to the extent reasonably possible, the identity of their customers as a best practice.
16. Advertising intermediaries should be encouraged to sign up to voluntary best practice schemes such as those run by the TAG and the 2018 EU MOU on advertising and IP rights.

About the Authors

Ardi Janjeva is a Research Analyst in RUSI's Organised Crime and Policing team. His research spans numerous areas within organised crime and national security, including the application of emerging technologies for use in national security and law enforcement contexts, the intersections between cybercrime and fraud, and intellectual property crime.

Alexandria Reid is a Research Fellow in RUSI's Organised Crime and Policing team, where she focuses on environmental security, illicit trade and related illicit financial flows. Alexandria is also Deputy Director of the Strategic Hub for Organised Crime Research at RUSI.

Anton Moiseienko is a Research Fellow in RUSI's Centre for Financial Crime and Security Studies. His research covers a range of subjects that include the laundering of the proceeds of cyber-dependent and cyber-enabled crime and money-laundering vulnerabilities of online businesses.