

At a Glance: Taking the Profit Out of Intellectual Property Crime

KEY FIGURES



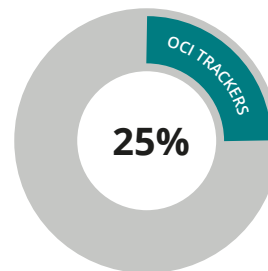
The film and TV sector generated £20 billion for the UK economy in 2018



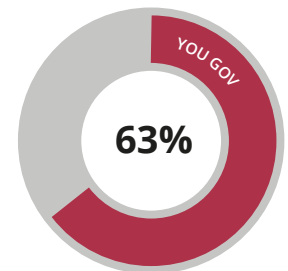
The UK's creative industries contributed two million jobs in 2018



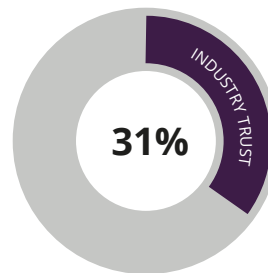
Total years of prison time handed out to 25 illegal IPTV suppliers between October 2017 and November 2020 in the UK



Average level of infringement in the UK population



Would recommend pirate services to friends and family



Pay to access infringement content via box or app

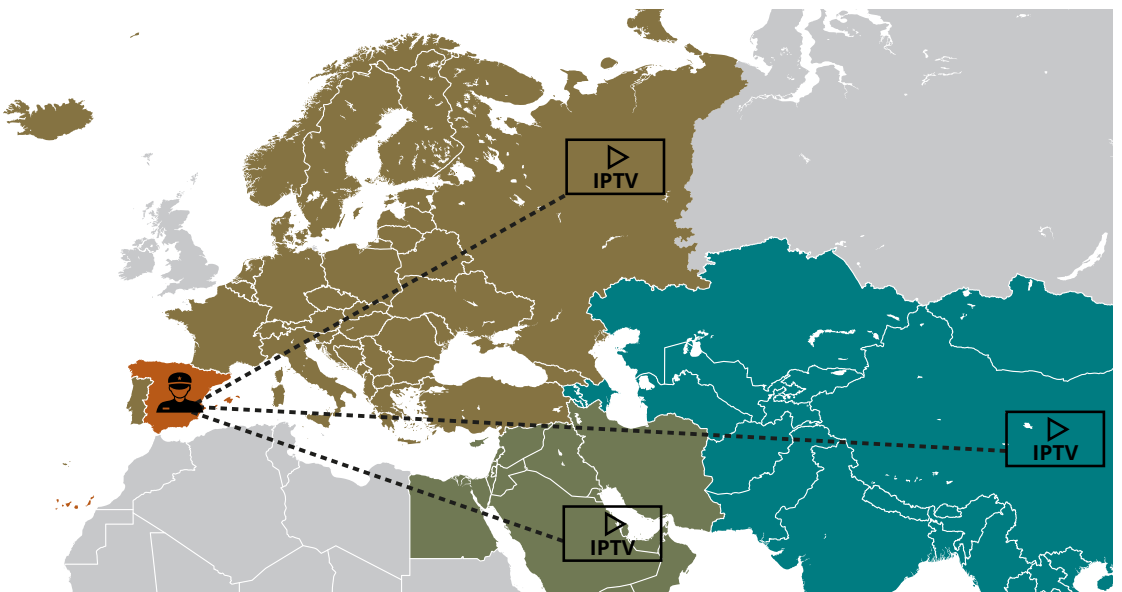
Of which fall victim to fraud

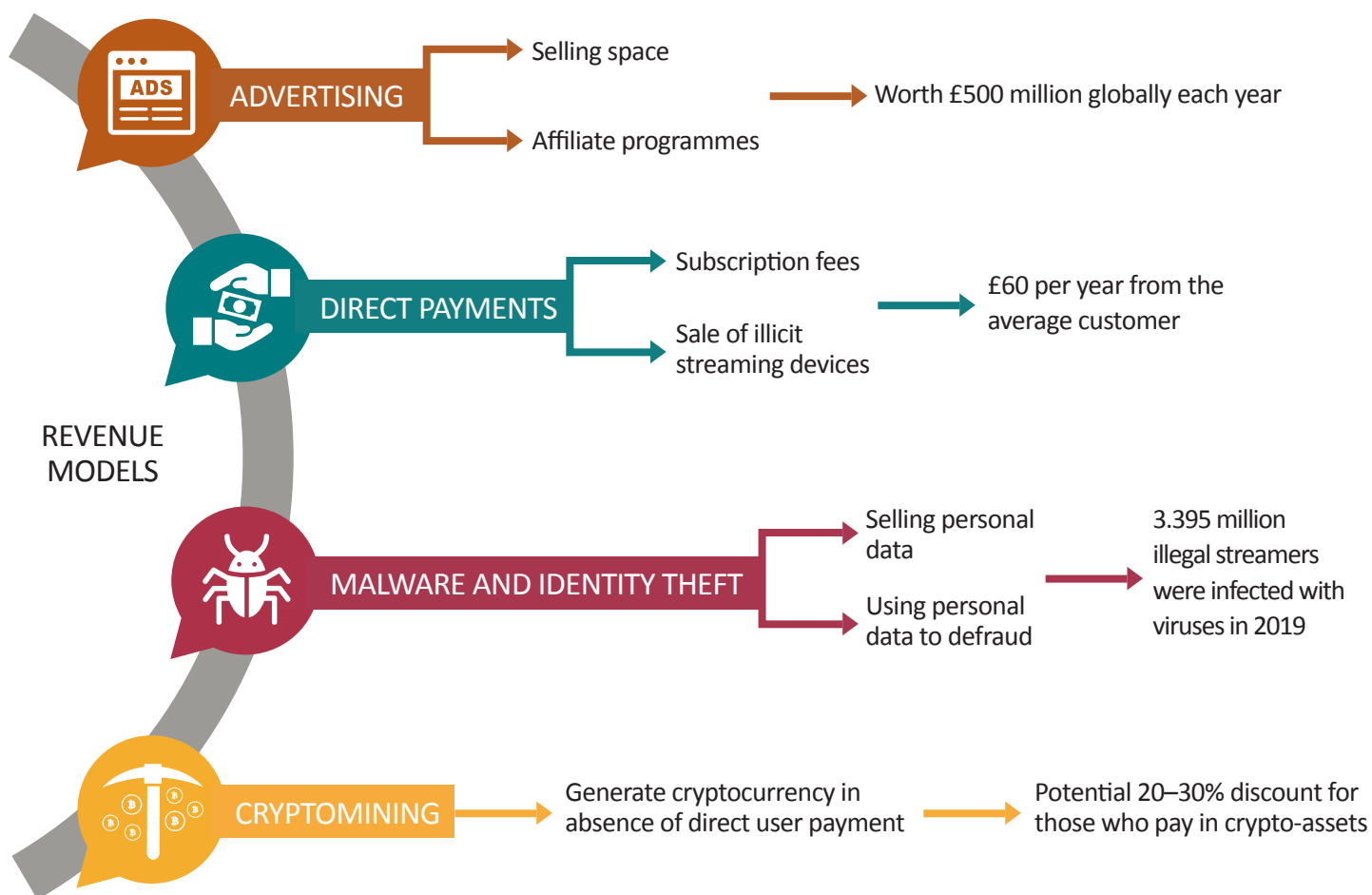
Of which are charged multiple times

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. On 3 June 2020, law enforcement authorities across the EU carried out 15 house searches, arrested 11 individuals and interrogated 16 others for their possible involvement in the illegal scheme. The actions resulted in the seizure of €4.8 million, including properties, cars, luxury watches, cash, cryptocurrencies and electronic equipment:

€4.8 million

in seizures including





RECOMMENDATIONS

- 1 Public-private partnership:** Sharing intelligence across law enforcement and the private sector
- 2 Reducing monetisation opportunities:** Greater use of pirate website lists among financial institutions
- 3 Access and demand reduction:** Implement ‘know your business customer’ requirements for online service providers to record and verify customer identity
- 4 Payment disruption:** Public-private partnerships should engage with acquiring banks, payment service providers, card payment schemes and crypto-asset service providers
- 5 Strengthening financial investigations:** Resourcing for a whole-of-system response coordinating agencies across government and activating investigative skills across the UK’s serious and organised crime policing network

‘There is great promise in the UK’s championing of a “follow the money” response to IP crime, but current efforts have not greatly reduced the ability to make significant criminal profit from piracy. Changing this requires demand-side action, 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 enabling consumers’ access to that content and criminals’ ability to receive payments for it’.

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.

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 cyberlockers⁵ 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

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

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. 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.

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.

The views expressed in this publication are those of the authors, and do not reflect the views of RUSI or any other institution to which the authors are or were affiliated.

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



This work is licensed under a Creative Commons Attribution – Non-Commercial – No-Derivatives 4.0 International Licence. For more information, see <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

The accompanying report for this document is: Ardi Janjeva, Alexandria Reid and Anton Moiseienko, 'Taking the Profit Out of Intellectual Property Crime: Piracy and Organised Crime', *Whitehall Report 4-20* (March 2021).

Sources for pp. 1–2 include: 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>; 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/ukscreative-industries-contributes-almost-13-million-to-the-uk-economy-every-hour>; IPO, *Online Copyright Infringement (OCI) Tracker*, 9th Wave (London: The Stationery Office, 2019); YouGov, 'The Impact of Pirated Streaming Services in Britain', March 2017; data provided by FACT; Industry Trust, 'Quarterly Tracker: Quarterly Research into the GB Population's Usage of, and Attitudes Towards, Infringement Methods', June 2020; 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>; 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; Crimestoppers, 'Streaming Online – Know the Risks', <https://crimestoppers-uk.org/keeping-safe/online-safety/streaming-online-know-the-risks>; authors' interview with a foreign law enforcement policy official, 31 July 2020.

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)