

# SportsPro REPORTS

September 2021

# Content protection and the fight against streaming piracy

# Contents

- 3. **Foreword**
- 4. **PART ONE: Inside the fight against streaming piracy**
- 5. Piracy: the big picture
- 7. Understanding consumer triggers
- 11. Technological solutions for anti-piracy
- 19. The legal challenge
- 22. Case Study: Premier League and La Liga's Mobdro takedown
- 23. 'There's no single solution': The BelN guide for thwarting piracy
- 27. Case Study: How Uefa tackled piracy during Euro 2020
- 29. **PART TWO: From cost centre to revenue opportunity**
- 33. Why consumer trust matters
- 35. Counting the cost of cyber crime
- 37. Quantifying the value of content protection
- 38. Targeting the 'converter cohort'

SP



# Foreword

**Video content remains the sports industry's most valuable asset, and it is under threat like never before. From password sharing and illegal streaming devices to industrial-scale piracy, sports rights owners face a significant technological, legal and business challenge to protect their content on its journey to legitimate licensees and subscribers.**


Today, rights owners have a central role to play in safeguarding their intellectual property, yet the fight against illegal live streaming is a battle they

cannot win alone. Only through collaboration with technical specialists, law enforcement, broadcasters and other relevant stakeholders can content owners expect to navigate a complex and ever-changing piracy landscape whilst effectively protecting their bottom line.

Of course, no anti-piracy programme can be 100 per cent effective. But implementing the right content protection strategy is critical for organisations across a sports media industry that is increasingly shifting to digital-first, direct-to-consumer business models. And it is not only video content that must be protected. In



today's digital ecosystem, mobile apps, online payments and sensitive user information must all be securely guarded, not only to protect all-important income but also to maintain brand reputation and trust among consumers.

This report, produced by SportsPro in collaboration with Verimatrix and Intertrust ExpressPlay, delves deeper into the never-ending fight against illegal streaming, IP theft and other forms of cyber crime, whilst also presenting some of the innovative solutions for transforming the threat of piracy into a revenue growth opportunity. 

SP


# PART ONE: Inside the fight against streaming piracy



# Piracy: the big picture

**Streaming piracy is by no means a new scourge, nor is it purely a sporting one. But with thousands of illicit services worldwide it is a pervasive problem that has spawned a hugely profitable business. Indeed, the lucrative nature of the industry has long rendered broadcasting and streaming of sports and entertainment content a magnet for criminal activity.**

Evidence indicates that the illegal transmission of sports events online causes significant economic damage to the sports sector, resulting in losses in subscription and advertising income. According to [an early 2021 study conducted by Ampere Analysis](#), sports rights owners are missing out on more than US\$28 billion in revenue each year as a result of piracy. Further research [carried out by the Digital Citizens Alliance](#) found that pirate subscription OTT services have grown into a billion-dollar industry in the United States alone.

While the problem exists in just about every sport and every country on the planet, rates of piracy are generally proportionate to the popularity of the properties being targeted. In English soccer's Premier League, which owns some of the most lucrative broadcast rights in sports and also - not coincidentally - runs one of the industry's most comprehensive anti-piracy programmes, 300,000 live match streams were blocked or disrupted in the UK alone during the 2019/20 season. 

## TRIPLE THREAT: three types of streaming theft

### Piracy sites, apps and devices

This includes any service streaming illegal content through an unauthorised website, mobile app or games console, or other hardware devices like a modified set-top box. Think First Row Sports, Mobdro and 'fully loaded' Kodi boxes.

### Credential selling and password sharing

This includes both casual sharing, where people share credentials with their family and friends as a goodwill gesture, and fraud, where hackers obtain compromised credentials on the dark web and sell them on marketplaces for a lower price than a legitimate subscription.

### Restreaming

This is where bad actors steal cable and satellite feeds for redistribution or rip online streams from legitimate OTT services. Redistributed streams are often further redistributed, sometimes through automated means.

SP



Sports service providers and rights holders are missing out on up to **US\$28.3 billion** in new revenue each year as a result of piracy

[\(Ampere Analysis\)](#)



OTT sports streaming services would stand to gain **US\$5.4 billion** by eradicating piracy

[\(Ampere Analysis\)](#)



**51% of sports fans** use pirate services to watch live sport on a monthly basis

[\(Ampere Analysis\)](#)

By 2023, overall revenue lost to pirates of pay-TV and non-pay-TV video is expected to exceed **US\$67 billion** worldwide

[\(Parks Associates\)](#)

In the US, **20% of broadband households** use a piracy device, app or website

[\(Parks Associates\)](#)

**54% of millennials** have watched illegal streams of live sports and a third admit to regularly watching them

[\(SMG Insight\)](#)

**20 million active subscribers** are paying to watch pirate content in Europe

[\(Ampere Analysis\)](#)

SP

# Understanding consumer triggers

**Generally speaking, the growth in streaming piracy is a result of several interrelated trends, from the proliferation of broadband connectivity and the rise of social media to a younger generation that has grown accustomed to accessing content for free. In sports, however, there are several other factors at play.**

For many sports fans, restrictions on access to legitimate content are seen as a key motivator, with many leading properties have long transitioned their premium live content behind the paywall. Traditionally, complex contractual agreements that include geographical rights restrictions and exclusivity arrangements limit content access and availability. Then there is

the ongoing industry-wide shift from traditional linear broadcast models to subscription-based streaming and over-the-top (OTT) distribution, which has further ring-fenced and fragmented sports consumption whilst driving up competition and investments in content.

As well as restricted access, industry experts suggest the problem of illegal streaming also

SP

correlates with the cost of watching legitimate streams. One consequence of the ongoing proliferation of streaming services is that the rights to most premium properties are now split across an increasing number of platforms. That, in turn, has increased the risk of what has come to be called 'subscription fatigue', whereby consumers are being priced out of following their favourite sports by legitimate means because doing so requires an array of digital subscriptions.

By contrast, many paid-for illegal streaming services offer excellent value for money. Unencumbered by content acquisition costs, geo-restrictions and competition law, nowadays there are thousands of pirate services aggregating a broad variety of sports channels for a fraction of the cost of a legitimate cable or digital subscription. What's more, the quality, availability and reliability of these so-called 'super aggregators' has helped fuel their popularity among sports fans.

Where once pirate sites might have been dogged by pixelated streams, constant buffering and malware, many now feature broadcast-quality feeds and professional-grade interfaces. Even if intrusive advertising and malicious pop-ups do persist, a free stream that is at best satisfactory can be a more favourable option than paying for a legitimate, better quality one.

"I think there are some cases where it's not about finding free content - it could just be that it's so much easier to use the illegal services," says Martin Bergenwall, the senior vice president of product management at Verimatrix. "You have to make the service that you offer really easy to use, you have to look at the user experience, and at the same time you need to fight the piracy to make sure that there aren't illegal services evolving that have the ability to offer something that is really smooth and slick.

"Pirates can do that because they don't pay for the content, so they can just focus on the user experience. That's why you need the anti-piracy services to make sure that that doesn't happen. There will always be illegal streams but when it's on a major industrial scale, it's a big problem."

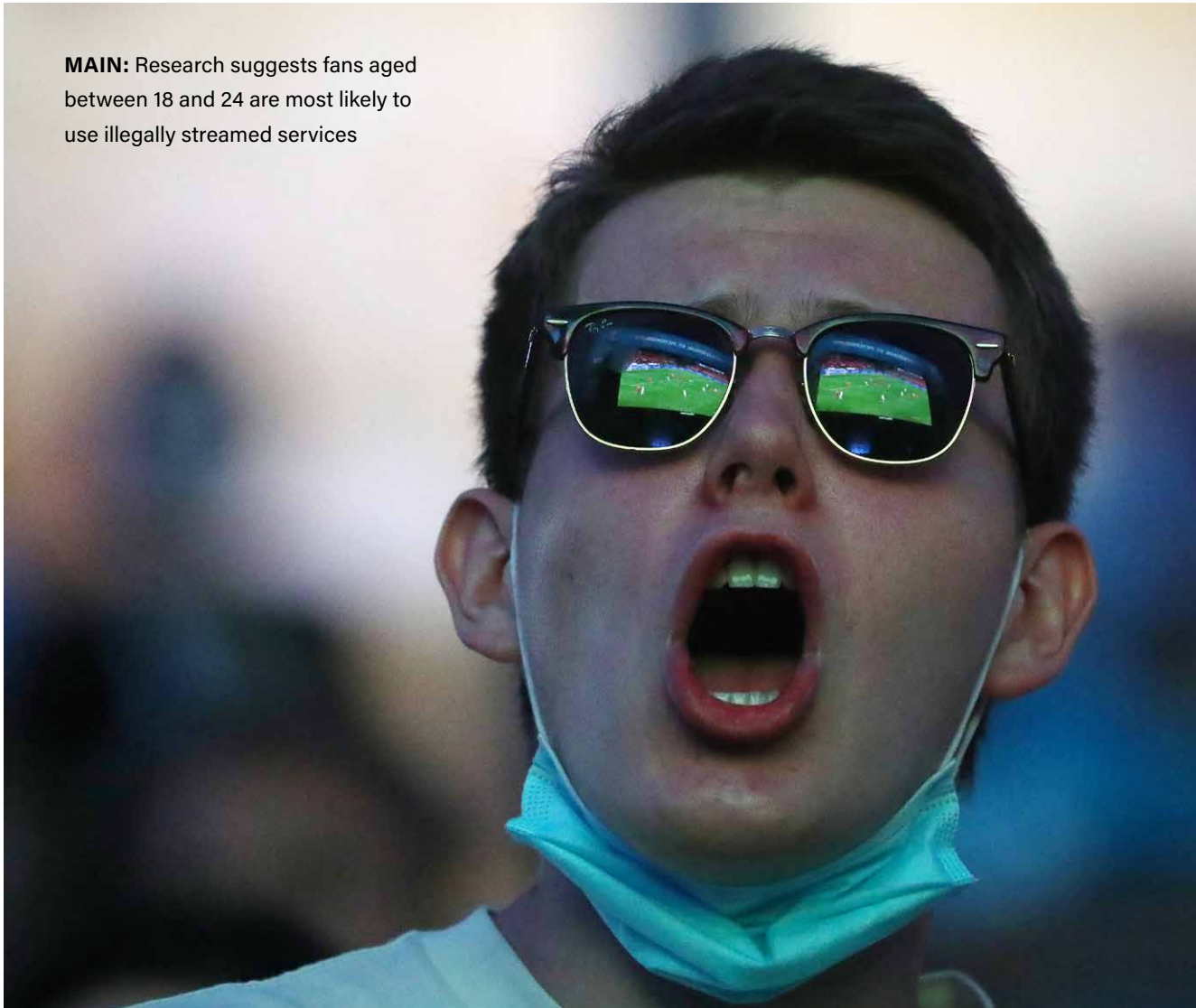
During the coronavirus pandemic, the need to understand audience behaviour has only taken on added significance. After lockdown measures came into effect in March 2020, the demand for all types of content surged, yet the restrictions placed on attending live events proved a double-edged sword. Not only did it bring about new opportunities for developing subscription models and growing audiences for streaming services, it also created ideal conditions for illegal streamers to operate. ▶

**A free stream that is at best satisfactory can be a more favourable option than paying for a legitimate, better quality one.**



SP

**MAIN:** Research suggests fans aged between 18 and 24 are most likely to use illegally streamed services



Indeed, across sports, the expectation was that empty stadiums and the closure of pubs and bars would lead to a piracy boom, and on evidence that seemed to be the case: in January 2021, for example, research from finder.com found that almost 1.9 million people in the UK admitted to illegally streaming Premier League games in 2020.

Interestingly, the study noted that the figures were likely to have been driven up by the controversial, short-lived scheme to make some matches available via pay-per-view (PPV) for the first time on Sky Sports and BT Sport. It also found that there was a correlation between younger viewers and illegally streamed Premier League matches. Gen Z fans - those aged between 18 and 24 - were the most likely to use illegally streamed services, with six per cent admitting to doing so. This was closely followed by five per cent of millennials and three per cent of Gen X viewers in the 40 to 54 age bracket. By contrast, only one per cent of those aged 75 and above said they had watched Premier League matches illegally.

A further factor enabling the consumption of illegal streams is the growing prevalence of virtual private networks (VPNs) and proxy servers. According to a survey by Global Web Index, approximately three in every ten internet users ▶

SP

uses a VPN service, with more than half of them admitting their primary objective is to access territorially restricted content such as live sports.

What's more, cybersecurity firm Webroot recently found that 92 per cent of illegal streaming sites used for pirating sports content over a single weekend were promoting a range of Bitcoin and mobile app scams, as well as containing malware threats. Yet despite the risks associated with illegal streaming, such as fraud, identity theft and the possibility of

criminal prosecution, the practice has become more widespread and increasingly socially acceptable. According to Parks Associates, 20 per cent of broadband households in the US use a piracy device, app, or website. Another report conducted by SMG Insight in 2017 found that 54 per cent of millennials have watched illegally streamed live sports and a third admit to watching them regularly.

Educating consumers about the illegality and hidden dangers has thus become a key focus

of anti-piracy programmes. In December 2020, for instance, the Premier League sought to do just that when it launched the second phase of its anti-piracy campaign in Malaysia and Hong Kong. Run in collaboration with broadcast partners Astro and PCCW, the 'Boot Out Piracy' campaign aims to highlight the dangers that illegal streams pose to fans, including data theft and malware, as well as emphasising the poor viewing experience through broken links and increased latency. <sup>SP</sup>

**92% of illegal streaming sites promote a range of Bitcoin and mobile app scams**

**RIGHT:** The Premier League's 'Boot Out Piracy' campaign aims to emphasise the superior viewing experience offered by legitimate services



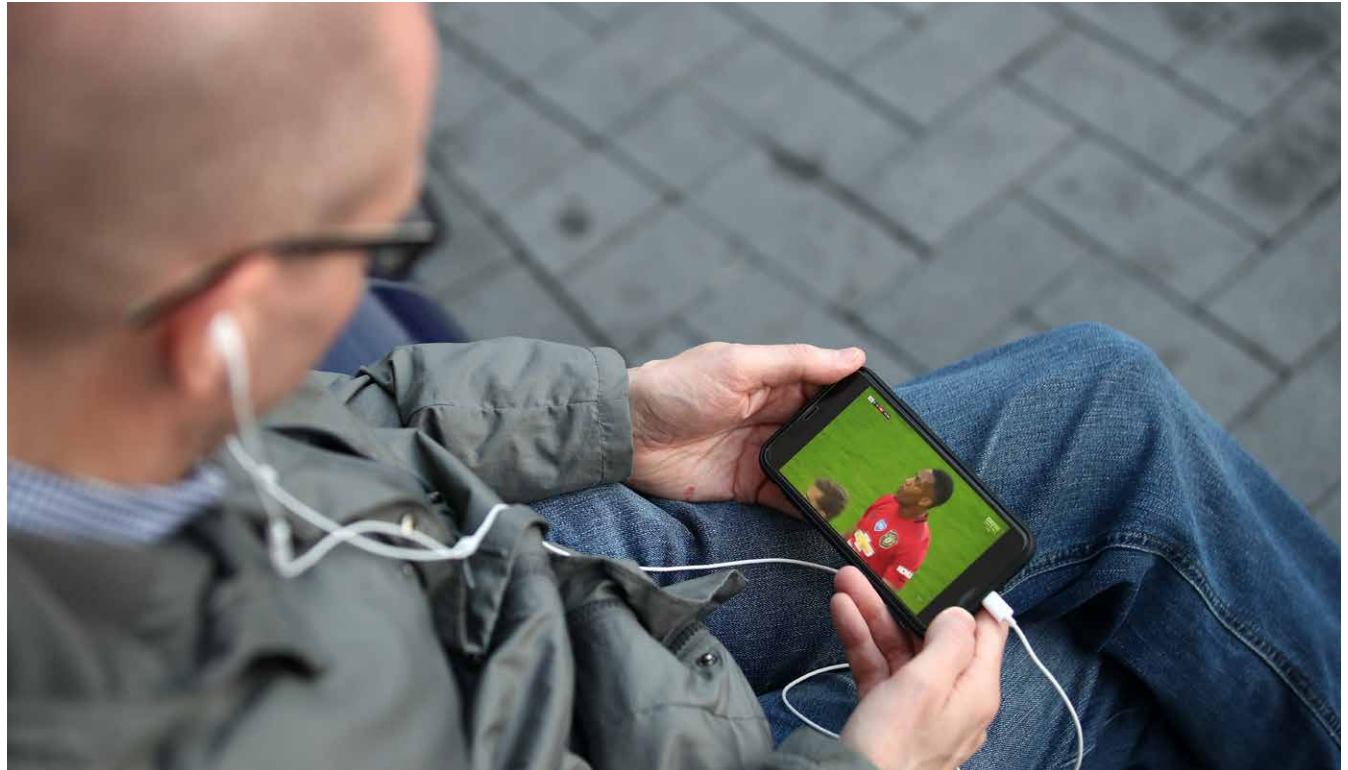
SP

# Technological solutions for anti-piracy

**An effective anti-piracy strategy combines a range of technological solutions for securing content and detecting copyright infringement, each of which works in tandem to deliver end-to-end service protection.**

“Content protection has to be part of the overall service protection strategy,” says Ali Hodjat, vice president of marketing at Intertrust ExpressPlay. “It’s not just about content, it’s the overall service that needs to be protected because it ties to revenue.

“Overall, to protect the revenue you need to protect the service, which means you need to protect the content, your devices, and your applications. Above all, you need to have a plan for how to respond to piracy before it happens. A well-defined anti-piracy strategy must be an integral part of the development of a premium live sports streaming service.”



SP

# Digital Rights Management (DRM)

Designed to encrypt content during transit to the consumer's player, a DRM service protects the legitimate, authorised path from the stream origin to the point of consumption before a breach occurs. DRM works by managing content encryption and defining usage permissions for the content, as well as enforcing those policies within the playback device. A DRM service ensures only legal users can decrypt the content, issuing an access key to the authenticated client upon request. ▶



SP



**LEFT:** Intertrust  
ExpressPlay's Ali Hodjat and  
Manas Mati

**“There is zero tolerance for latency on live content. Anything that adds latency is going to be an issue.”**

“Everything starts by protecting the content and having the correct authorisation or rights management for paid subscribers - that’s where DRM comes in,” explains Hodjat. “DRM protects the content itself and the rights for the users who pay for it. Intertrust co-founded the first and so far only open-standard DRM for media and entertainment, called Marlin, back in 2005. Marlin is governed by the Marlin Community. The Marlin Trust Management Organization (MTMO) is the operational entity that grants commercial licenses for Marlin technology.”

When it comes to implementing content protection in a world of constantly increasing device fragmentation, a flexible multi-DRM

service is key. With content being consumed across a growing array of devices and multiple operating systems, each of which may employ their own embedded DRM client, implementing a cloud-based solution that spans them all is critical.

Another key objective is instant scalability, which is especially important in the context of live sports, where the vast majority of subscribers are accessing the content at the same time and will not accept excessive delays or poor streaming performance. Again, this objective is best achieved through a cloud-based multi-DRM service.

“Making sure every paid subscriber receives their DRM licence at the same time in order

to watch the live game becomes the key requirement,” adds Hodjat. “And then the second important factor is latency. There is zero tolerance for latency on live content, so anything that adds latency is going to be an issue. DRM licence delivery and content encryption for live streaming needs to be implemented without imposing any discernible latency.”

To minimise latency within the delivery workflow to just a few milliseconds, both the content and DRM licences are typically processed through one or more Content Delivery Networks (CDNs). Real-time analysis of DRM licensing provisions via a DRM analytics dashboard also enables operators ►

SP

to constantly monitor service failures, the number of requests being made, and the level of latency associated with each DRM.

Today, several cloud-based multi-DRM services that support all platforms and formats exist in the market. In Asia, for example, the [Intertrust ExpressPlay multi-DRM service](#) is utilised by large-scale operators such as SonyLIV, Hotstar, iQiyi and Tencent to protect their live and on-demand content, including streaming coverage of major sports leagues and events. Another example is BT Sport in the UK.

“All of these large platforms don’t limit themselves to browsers or certain operating systems,” notes Manas Mati, general manager of Intertrust’s ExpressPlay subsidiary. “They want to ensure that they are on Roku, Chromecast, Amazon Fire Stick and so on, so there are a number of client device platforms

where they need content protection. This is where the cloud-based ExpressPlay multi-DRM service really shines by supporting all those platforms and more.

“But the most important factor is that unlike with library-based content, live sports has unique challenges. For large companies like SonyLIV, they plan months beforehand. They get a group of customers and vendors together and plan a strategy, including how likely traffic is going to spike, and we participate in those discussions. Our guys work with them to scale up and scale down, monitoring and managing the moments where there are audience spikes.”

Elsewhere Mola.tv, one of Indonesia’s largest OTT services, is secured by [Verimatrix’s Multi-DRM solution](#). Hosted via the Verimatrix Secure Cloud and leveraging a SaaS model, Verimatrix protects Premier

League soccer and other live sports content streamed by Mola.tv with optimised DRM capabilities that ensure decryption keys are kept safe and distributed at scale to only authorised users during games.

“The most important component of DRM is that it needs to be friendly,” claims Verimatrix’s Martin Bergenwall. “Tough enough to thwart the pirate’s endeavours but invisible to fans. Security cannot disrupt the viewing experience in any way.”

Adds Hodjat: “DRM is a component of content protection and it should be enforced all over. Now, there might still be piracy even if you use DRM, and that’s where we need to focus on content monitoring, takedown services and forensic watermarking. It reinforces the need to map out the right strategy for how to respond to piracy before it becomes an issue.”

**“The most important component of DRM is that it needs to be friendly. Tough enough to thwart the pirates but invisible to fans.”**

# The one-stop shop

for content protection and anti-piracy services



The ExpressPlay Media Security Suite consists of a cloud-based and studio trusted multi-DRM service, unique broadcast TV security, and comprehensive anti-piracy services.

## Intertrust ExpressPlay DRM™

Securing high-value streaming services

Cloud-based multi-DRM media monetization service for OTT streaming operators and content distributors. Scales to protect millions of concurrent viewers for major live events with a cost-effective and low latency solution.



## Intertrust ExpressPlay XCA™

Next-generation security for broadcast content delivery

ExpressPlay XCA is a cloud-based broadcast security service, based on open-standard Marlin DRM, which secures delivery of premium/UHD and hybrid DVB-OTT services to smart TVs without STBs or external security.



## Intertrust ExpressPlay Anti-Piracy™

Anti-piracy services for enhanced content protection

ExpressPlay Anti-Piracy and Watermarking service incorporates content protection that features online piracy monitoring and forensic watermarking for legal enforcement of live and VOD streaming services.



## Intertrust ExpressPlay DRM Offline™

Secure offline streaming solution ideal for travel and hospitality applications

ExpressPlay DRM Offline provides a multi-DRM solution for secure content delivery and playback in offline environments. It allows authorized users to gain secure access to premium and rights managed content.



Intertrust  
**ExpressPlay**®

Drop us an email for a no-obligation consultation at:  
[onestopshop@expressplay.com](mailto:onestopshop@expressplay.com)

[www.expressplay.com](http://www.expressplay.com)  
Telephone: +1 408 616-1600

SP

# Forensic watermarking, digital fingerprinting and content monitoring

**An important complement to DRM, a watermark is a unique, embedded overlay that identifies content ownership throughout the entire distribution process. Information such as the device IP address can be embedded in the video itself, at the point of origin, in the CDN during delivery, or within the player device. Typically, this information is not visible to the human eye but if a watermarked video is identified on an illegal stream, a detection mechanism can be used to determine its origin.**

“There are basically three ways to do watermarking,” explains Bergenwall of Verimatrix. “One is **distribution watermarking**. This would be when the Premier League, for example, gives out a football match to a broadcaster, they include a distribution watermark which is not unique to the user or end viewer, but unique to that broadcaster. So if that was leaked, they would know it came from that broadcaster.

“Then you have **client-side watermarking**, where the client that does the playback will

insert a unique identifier, like a subscriber ID, into the video. So before it’s displayed on the screen that watermark is inserted into the picture, and if you were to do a screen recording that can also be extracted.

“And then finally there is what is called **session-based watermarking**, specifically for streaming. Video streams are typically built out of small fragments of video layered on top of each other, so what session-based watermarking would do is build a unique ‘playlist’ where the stream that you receive is unique to you and it ▶

**RIGHT:** Martin Bergenwall, senior vice president of product management at Verimatrix



**“With forensic watermarking you can see who is the subscriber behind the piracy, you can alert them that you’ve caught them.”**



SP

**“You need to have a plan so that when you identify piracy you know what types of mitigations you should perform.”**



## VIDEO

Three techniques to strike out piracy  
SportsPro Live 2021

**Watch now**

can be traced back to that session, even if the human eye can't see that watermark."

In conjunction with watermarking, fingerprinting enables content owners to quickly identify their video and then take action to remove that stream, such as revoking the DRM key or the infringing user account. This process is supported by real-time monitoring services and web crawling tools that are used to detect pirated services and redistribution links.

Once the watermarking ID is extracted, the source can then be shut down. Disruption techniques can also be used to degrade the

quality of pirated streams by pixelating the feed or cutting the signal altogether.

Russian streaming service Okko Sports implemented Verimatrix Watermarking to assist in preventing unauthorised broadcasts of the Premier League, MLS, Italian Cup, Bellator and ATP 250 tournaments. Invisible to viewers, forensic watermarking helps gather real-time information about specific pirated content while also instantly blocking pirated broadcasts.

"A lot of times this gets lost in the conversation," says Hodjat. "As part of the overall end-to-end service protection, you need to

have a plan in place beforehand so that when you identify piracy you know what types of mitigations you should perform. There are ways to block devices or stop delivering DRM licences or issue takedown notices, even sending on-screen messages.

"As part of a DRM platform, you can send out messages to the subscriber. So if you see the content being pirated and with forensic watermarking you can see who is the subscriber behind the piracy, you can alert them that you've caught them. These are things that should be covered as part of how to respond to piracy."

SP

# Application shielding


**App shielding technology is intended to protect intellectual property and ensure legitimate software cannot be manipulated, modified or misused in any way. It works by obfuscating an app's binary code, making it more difficult for attackers to reverse-engineer, remove DRM keys and steal media.**

Hackers who target apps are able to exploit vulnerabilities in mobile software to spy on users and steal personal data. Since live streams are typically distributed through a variety of mobile, web and smart TV apps, end-point video players that are particularly susceptible to attacks require robust protection.

"We've seen examples where someone has taken a valid application and reversed engineered it to make unlawful modifications," says Bergenwall. "Maybe they insert their own advertisements, remove some of the checks to allow access to a broader audience, or just steal credentials and private information."

As Bergenwall notes, application shielding techniques are evolving in line with the growing need to strengthen app defences across a range of industries, not least financial services and other high-value environments like live sports.

"Sometimes there is a misperception that apps are standalone and you don't need to worry because content is secure in the backend," he continues. "But apps are extensions of the service. If you sign up to a service, it's not an independent instance; it's an extension of the whole video service. Apps typically feature APIs in the backend to retrieve the video and perform functions like user authentication, and if the apps can be hacked and modified, then it's basically a breach of that service.

"Even if you wouldn't store anything sensitive within the app, the app would have access to that sensitive information, which is stored in the backend." 



**ABOVE:** Social media apps have become enablers for live streaming

SP

# The legal challenge

**Taking down illegal live streams has been likened to a game of whack-a-mole: as soon as one pirate site is removed, another springs up in its place.**

Pirates aim to stay one step ahead of efforts to combat them and it can be likened to a constantly shifting arms race. The level of sophistication with which they operate has increased in line with the professionalisation and profitability of their services. Websites generally make their money by selling cheap ads which generate, say, a few dollars per 1,000 impressions, with combined revenues for pirated TV services estimated to have hit ten figures globally.

It is little wonder, then, that illegal streaming draws complex networks of hackers, distributors and organised crime syndicates who operate at an industrial scale. Many use circumventing tactics such as screen recording software, external camera recording, or HDMI capture devices. Some even employ advanced analytics to gather in-depth usage data and offer customer support services.

SP

# Technology alone may not be sufficient to block illegal services and the redistribution of live sporting events.

Given the complex nature and rising sophistication of these pirate networks, technology alone may not be sufficient to block illegal services and the redistribution of live sporting events. Besides the deployment of technological solutions like forensic watermarking, policing piracy demands collaboration among multiple stakeholders and a collective willingness to go after not just web domains and host servers, but the people behind them. That is often a drawn-out and costly undertaking to the extent that it simply cannot keep pace with the immediacy of the live broadcast environment.

Legal mechanisms for disrupting and removing illegal streams do exist, yet enforcing legislation is fiendishly difficult. Insufficient security and cooperation throughout the broadcast supply chain, coupled with a lack of consistent international copyright laws and legislation for enforcement, often means any attempts to stop the pirating of live streams prove almost futile.

Further complicating matters is the fact that social media platforms have become enablers for live streaming. Popular platforms such as Facebook, YouTube and Twitter, and 'linking sites' like Reddit, have only accelerated the illegal streaming industry's growth. In fact, over 41 million viewers watched illegally redistributed

streams during the 2018 Fifa World Cup via social media alone.

Nevertheless, there have been some notable legal victories across the industry. In 2017, for example, the Premier League obtained a high court injunction that compelled internet service providers to block pirate servers, thereby ensuring detected streaming sites would be blocked in the UK. The league has also taken legal action against some retailers for selling illegal streaming devices, while in March 2019 three men, who made more than UK£5 million selling illegal Premier League streams to over 1,000 pubs, clubs and homes, were jailed for a combined total of 17 years, some of the longest sentences ever for video piracy crimes.

Elsewhere, in June 2020, LaLiga won an anti-piracy ruling in Moscow to remove its content from three Russian websites that had been illegally streaming Spanish top-flight soccer matches, while that league has also secured successful rulings in Brazil, Mexico, Peru, Denmark, Senegal, and Indonesia.

At the same time, concerted efforts to lobby policymakers have gathered pace in recent years, with the Sports Rights Owners' Coalition (SROC), an informal group of 50 international, European and national sports bodies, having placed anti-piracy at the top of its agenda. ▶

SP

In May, the group publicly commended the European Parliament for voting to adopt its resolution on the 'Challenges of sport events organisers in the digital environment' - a development it described as 'a major step forward for the protection of live content more broadly, but for live sports content in particular.'

'The resolution recognises the unique nature of live content and the fundamental need to

move quickly to stop piracy,' read the group's statement. 'The call for an immediate, and in any event no later than within 30 minutes, removal of infringing broadcasts would have a hugely positive and almost instantaneous impact on addressing live sports content piracy.'

'We now call on the European Commission to follow the European Parliament's recommendations and to introduce binding

targeted legislation without delay. Both the context and expected timeframe of the proposed Digital Services Act are out of scope to provide the necessary solutions. Time is of the essence in this process and our sector urgently needs specific and efficient remedies as piracy continues to grow and dramatically undermine the viability of the model and funding of European sport.' <sup>SP</sup>



SP

## CASE STUDY: Premier League and La Liga's Mobdro takedown

In March, the Premier League and La Liga secured another anti-piracy victory with the removal of the Mobdro mobile app, which was illegally streaming games from both top-flight soccer leagues.

The investigation into Mobdro, considered the world's largest pirate streaming app with more than 100 million users, began in October 2018 when the Spanish National Police received complaint reports from the Premier League, La Liga, the Football Association Pretoria and the Alliance for Creativity and Entertainment (ACE). A number of connected websites and platforms were then identified in Spain and Portugal with connections to servers in the Czech Republic.

The Spanish company behind the illegal activity earned its profits through advertisements and were able to sell user information to a company related to botnet and distributed denial-of-service (DDoS) attacks. Investigators estimate the overall illegal profits generated by the operation totalled more than €5 million (US\$5.9 million).

Europol, the European Union's law enforcement agency, supported the Spanish National Police in the dismantling of the criminal group. This resulted in three house searches, four court orders to take down domains, 20 web domains and servers blocked, and four arrests. Bank accounts were also frozen and a server was taken down in Portugal.



**ABOVE:** La Liga collaborated with Spanish authorities to remove the Mobdro pirate streaming app in early 2021

SP

## 'There's no single solution': The BeIN guide for thwarting piracy

**Multinational pay-TV network BeIN Media Group continues to spearhead the fight against broadcast piracy around the world. In sports, its notorious case against BeoutQ, the Saudi Arabia-based pirate operation that began bootlegging BeIN's licensed content in 2017, has been well-documented, prompting widespread condemnation from governments and sports organisations.**

As part of its efforts to tackle piracy and protect its investments in sports rights, BeIN works closely with other industry stakeholders across its various markets. In France, for example, the broadcaster was a central force in creating the Association for the Protection of Sports Programmes (APPS) in 2018. That body, which now includes Canal+, Eurosport and other French broadcasters, aims to fight against all forms of content piracy, and earlier this year it successfully lobbied the French National

Assembly to adopt legislation that gives rights owners and broadcasters significant new powers to secure injunctions to block, remove or de-reference pirate websites and servers that illegally distribute live sports content.

Here, Cameron Andrews (above), legal director, anti-piracy at BeIN Media Group, outlines some of the legislative tools that exist for tackling illegal operators and explains what more can be done within sport to diminish the threat of content piracy. ▶



**"It's like a drugs network, really. That's the best analogy I can give: a very sophisticated distribution network."**



SP



**LEFT:** Saudi Arabia-based pirate operation BeoutQ began bootlegging BeIN's licensed content in 2017

### **Why is it so difficult for sports rights owners to police piracy and bring perpetrators to justice?**

*It's such a big problem because the internet makes streaming piracy so easy. There has been an explosion of new, legitimate streaming services, but in parallel, and probably in front of all that, the pirates have already been making use of that technology to create an ecosystem and infrastructure to illegally restream TV channels.*

*Today, that has really exploded and there's a whole pirate ecosystem that sits underneath it. Here I'm talking about pirate IPTV services, which is the real threat to the industry. There are certain pirates at the bottom of the chain who source and stream the content, and others who aggregate the channels, and then layers of resellers and restreamers who supply this on to consumers.*

*It's a very clever system that they've built. There's a platform that sits behind it and they're able to do it very successfully because the internet makes it easy for them to be anonymous, it makes it very easy for them to reach their customers and to market what they're doing, and the law doesn't really make it very easy for rights owners to tackle it.*

### **What successes have you seen in sports when it comes to bringing pirates to justice?**

*There have been some successes over the last year or two and I think they're great and it's having an impact. I think there is a growing recognition among major sports rights owners of the size of the problem and the threat that it poses to the industry. We would call out the*

*Premier League and LaLiga, for instance, as doing a lot in this area.*

*But the issue is the size of the problem. It's very easy for the pirates to just reorganise, so you'll see a big action happens and a pirate network will be taken down, but very quickly the pirates recover. They will move to other servers in another country, or the resellers and the restreamers will just very quickly switch to another source to get the same content.*

*It's like a drugs network, really. That's the best analogy I can give: a very sophisticated distribution network. You've got suppliers or manufacturers, those who are copying the channels, right at the bottom of it. They are very organised and specialised in what they do. In our case, we know some of them are located* ▶



SP

**“I do think the sports industry has a long way to go. As an industry, not that much is known about who is behind all of this.”**

*in countries where it's very difficult to take any action against them. Then you have aggregators above that, and then resellers and restreamers, so it's a kind of spider's web.*

***Does more need to be done within sports to come together and, as an industry, collectively lobby lawmakers for tighter controls and tougher punishments?***

*Certainly there are coalitions that come together to tackle a particular issue, so when you look at some of the big cases they will involve various parties, rights owners and broadcasters, and that's really good. I think those efforts are picking up speed and there are certainly more of them than there were when we first started working on this.*

*But I do think the sports industry has a long way to go. As an industry, not that much is known about who is behind all of this. There's still, particularly for sports, an awful long way to go in discovering exactly how this works and who's behind it. If you compare the effort that the film and TV industry puts into tackling piracy, the way they've organised themselves and how much they're spending - I'm thinking of things like ACE, which is the Alliance of Creativity and Entertainment - there isn't really an equivalent in sports.*

*You've got some key rights owners who are doing good stuff and coming together in loose coalitions from time to time, but there isn't an overarching industry body that's tackling this, and I think that's really what has to happen. Rights owners need to dedicate a portion of their revenue to tackling piracy, they need to organise, they need to cooperate much more closely with their licensees, start taking this really seriously, and have an industry-wide strategy for tackling it.*

***Would you say the need to strengthen legislative solutions for tackling piracy is more pressing today than advancing technological ones?***

*There's no single solution; there is no one thing that will bring piracy back to tolerable levels. There's probably four things that need to be pursued in tandem, and rights owners play a leading role in all of that.*

*The first one is technology - watermarking, for instance, and stronger security. If content leaks from one licensee's platform, the global nature of the internet means that it affects all other licensees equally. If you've got one broadcaster with weak security, then we can all suffer from that. Rights owners sit at the top of the tree there, and I think mandating and enforcing*




*stronger security standards is a very important part of what they should do.*

*Another area that is becoming really important is ISP blocking. What you do - and it depends on the country - is you get either administrative or court orders requiring that internet service providers block their customers from being able to access pirate websites and servers that are serving up the pirated streams. This is a big part of what the Premier League is doing in the UK, and they are looking to do that in some other countries. LaLiga is pursuing it and we're doing it in countries where we can in MENA as well.*

*The third thing is what we call takedown notices, which is really about the internet companies that are facilitating the piracy. Pirates can't do this on their own, they have to buy the services of legitimate companies to both do the streams and promote their services. So there are a lot of legitimate companies involved.*

*The way we try to tackle that is identify them and send them takedown notices requesting that they withdraw services from the pirates. The law doesn't really help us very well at the moment because those internet companies get a very high level of legal immunity from liability for what their customers are doing.*

*For instance, there's no requirement that an internet company has to respond to a takedown notice within the timeframe of a live game, so it's not a particularly effective tool at the moment for dealing with live sports piracy. But it's really where the key lies because if the internet companies control the backbone for all of this, they're the ones that could make it so much harder for the pirates to operate.*

*The fourth one is the old-fashioned investigation and legal prosecution. That, in itself, won't stop piracy but it is important to send a message, deter people from doing it, obtain compensation and break the backs of these pirate networks. *

SP

## CASE STUDY: How Uefa tackled piracy during Euro 2020

One of the most popular sports events on the planet, soccer's European Championship is watched by millions of fans across the globe. Worryingly, though, many of those fans access match coverage through illegitimate services rather than officially licensed broadcast partners.

Each edition of Europe's flagship national team tournament generates well over €1 billion for governing body Uefa through the sale of media rights. That income is vital for supporting all levels of the European game, so protecting this all-important revenue stream requires a robust, multi-stakeholder approach.

For this summer's Euro 2020, Uefa continued its 'end-to-end' anti-piracy programme covering all the main forms of live and recorded pirated content, including online streams distributed via social media platforms, illegal IPTV services, unauthorised apps and 'linking sites'. As well as sending pre-emptive copyright notices to known pirate platforms of concern ahead of the finals, the body oversaw a coordinated

monitoring and enforcement effort in conjunction with its broadcast partners and other stakeholders.

During the tournament itself, thousands of takedown notices and cease and desist letters were sent to infringers and their enabling service providers. Infringing services were also de-listed from major search engines and pirate apps removed from popular stores. Alongside those efforts, Uefa actively engaged with the operators of the main social media platforms, such as Google, Facebook and TikTok, to reduce the ability for pirates to capitalise on the vast reach of their services.

Those efforts were not in vain. Days after the tournament's opening match, a Uefa-supported operation in Italy dubbed 'Euro Strike 2020' saw the Guardia de Finanza, which is primarily responsible for dealing with financial crime and smuggling in the country, successfully block more than 600 illicit services that were unlawfully streaming matches.



**ABOVE:** Italian authorities blocked more than 600 illicit services that were unlawfully streaming Euro 2020 matches

Security that's  
leveling up  
mobile gaming?  
Amazing.

 verimatrix™

Deliver amazing

[See how](#)



SP

# PART TWO: From cost centre to revenue opportunity

A silhouette of a person operating a camera on a scaffolding structure against a blue sky. The person is standing on a platform, and the camera is mounted on a tripod. The scaffolding is made of metal poles and cross-braces. The background is a clear blue sky with a dark silhouette of a mountain range on the left side.

SP

**Sports organisations of all kinds are rethinking business models and undergoing some form of digital transformation. Besides creating dedicated web and mobile apps, a growing majority of rights owners have launched owned and operated direct-to-consumer (DTC) streaming services and embraced emerging means of revenue generation, such as ecommerce, online betting and esports.**

This shift in strategy requires a simultaneous shift in thinking when it comes to content protection and anti-piracy. In the era of traditional linear TV, rights owners simply struck a deal with a broadcaster for a guaranteed rights fee and were less inclined to worry about what happened to their content. Today, as the distribution model has shifted towards DTC and online streaming, the challenge of protecting content and revenue is a chief concern.

Evidence suggests that, proportionally, digital services are affected by piracy more than any other revenue stream. In theory, as more sports content owners shift to OTT distribution, that threat to the bottom line only grows.

“The biggest thing that we are seeing, when we talk to traditional customers like the broadcasters, they have been in the TV business for years and they have a certain way of doing things,” notes Bergenwall. “When ▶



**Proportionally, digital services are affected by piracy more than any other revenue stream.**

SP



**“We work closely with customers to deliver the right layers of security ahead of launching the service, which is critical.”**

[www.sportspromedia.com](http://www.sportspromedia.com)

we talk to a sports league or team that wants to set up a service and monetise their own content, they have different expectations, and may not have a deep understanding of security requirements, so their needs are different.

“Time to market is important, but also user experience and friendly security. They don’t want to worry about all the security parameters; they want to have a solution that is easy, and can get up and running quickly. It’s also really important that it can scale automatically; they can easily modify the solution if they get one million or 100,000 viewers. They just want a service that reacts to their needs and the demand. We work closely with these customers to deliver the right layers of security ahead of launching the service, which is critical.”

In the digital age, virtually all emerging revenue generation models rely heavily on an effective security strategy. Indeed, new means of monetisation offered alongside live streams naturally demand stronger defences. Likewise, software that underpins online esports tournaments requires robust protection, primarily to avoid cheating during gameplay, and in those instances app shielding - as discussed previously - is paramount.

But despite the critical importance of deploying advanced security solutions,



SP



## “It’s all about protecting service revenue for the streaming platforms.”

across the sports industry such measures are often seen as a cost rather than an opportunity to generate revenue. To some extent that is understandable. At a time when more and more rights owners are investing heavily in launching streaming services and acquiring subscribers, anything that adds further expense, such as implementing robust content protection, is generally not prioritised until it is too late.

Still, the opportunity inherent within the growing problem of piracy is becoming increasingly clear. As Intertrust’s Hodjat explains, any investment in anti-piracy measures should be viewed as a way for rights owners to re-capture lost revenue, achieve customer growth

and reduce churn by converting illegal streamers into legitimate, paying subscribers.

“It’s all about protecting service revenue for the streaming platforms,” he says. “While DRM has always been mandated we’re now seeing forensic watermarking increasingly becoming enforced through their license agreements.

“If somebody is starting a new platform with their own valuable content they might have ignored content protection technology at their own peril because they were in such a rush to launch their services. But then as they start to get subscribers they suddenly see their content popping up in unauthorised places and being restreamed illegally. The value of live content is

exceptionally high for the duration of the event and much less afterwards. So they need to think about how much revenue they’re losing to pirated live services including lost ad revenue since pirates gladly sell ad slots themselves with many advertisers led to believe they are legitimate service providers.

“Today, more and more operators realise that smart content protection strategies including anti-piracy services can pay off by converting viewers of pirated content to legitimate and paid subscribers. Rather than looking at content protection purely as ‘cost’, it can become a driver for increasing revenue, subscriber growth and profits. That’s really the bottom line here.” <sup>SP</sup>



SP

# Why consumer trust matters

**With many turning to digital technologies in order to keep their fanbases engaged, particularly throughout the Covid-19 pandemic, leagues and teams have been able to build two-way relationships with fans that go far beyond the match day experience. Yet those relationships rely on an organisation's fundamental ability to foster and maintain trust among consumers.**

According to Deloitte's recent fan engagement survey, 95 per cent of sports fans currently have some form of interaction with their favourite team or league during the off-season. Some 65 per cent of fans say they want to receive some form of content from their team at least monthly during the off-season, while those who engage even just once a month in the off-season spend 40 per cent more than fans who have no engagement.

Satiating this appetite for content year-round is key for business growth but, as Deloitte notes in its '2021 outlook for the US sports industry', sports organisations must put the security of fan connections and data at the centre of their digital strategies in order to maintain trust. Doing so not only helps boost customer satisfaction and protect brand reputation, but it also minimises the risk of cyber attacks and ultimately safeguards revenue. ▶

SP

"If you don't have proper security, it can cause brand damage," says Verimatrix's Bergenwall. "I've been in the security industry for 20 years and I've seen a lot of really good security solutions that deliver the higher standard of security at the expense of the user experience. It's so important for service providers to take into account the user experience for their customers."

Sub-standard security solutions are those that detract from the user experience, adding latency to the video stream or requiring repeated authentication after log-in. As Bergenwall notes: "Good security is something you don't see." <sup>SP</sup>



**"It's so important for service providers to take into account the user experience for their customers."**

SP

# Counting the cost of cyber crime

**By 2023, according to research conducted by Statista, mobile apps may generate nearly US\$935 billion in revenue, so it is clear to see why, much like streaming piracy, cyber attacks against apps are on the rise. With increased reliance on these apps and ever-growing customer traffic, cybersecurity is now of paramount importance.**

According to the UK's National Cyber Security Centre (NCSC), cyber attacks against sports organisations are very common. In a study published in July 2020, some 70 per cent of sports organisations surveyed reported experiencing at least one attack per year, which is significantly higher than the average across UK business.

The study revealed that almost all sports organisations have a website, social media account, and hold digital records containing personal information about customers, staff and volunteers. Over 80 per cent of respondents also had online business systems and offered customers the opportunity to make bookings, payments or purchases via the internet. ▶




**Sports organisations conduct a lot of activity online and the vast majority hold personal information on customers/employees**

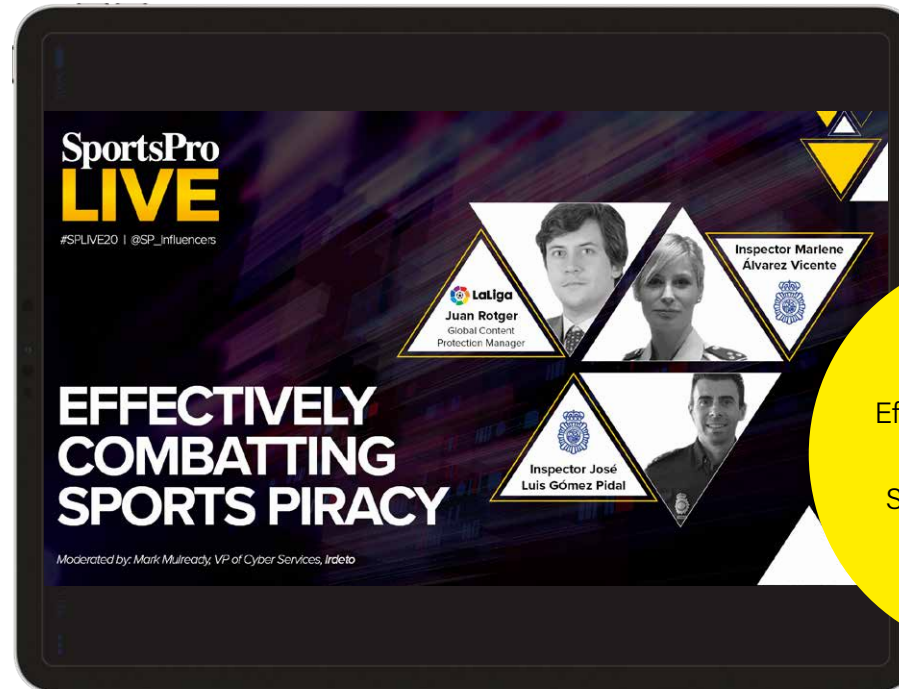
## Which of the following if any does your organisation currently have or use?

Accounts or pages on social media sites	96%
A website or blog	95%
Personal information about your (customers/beneficiaries/service users) held electronically	95%
Personal information about your employees held electronically	95%
Email addresses for your organisation or its employees or volunteers	93%
Internal online business systems	88%
The ability for customers to order, book or pay for services online	82%
A systems/database for sharing confidential, medical or performance data (players or athletes)	77%
An online bank account your organisation or your clients pay into	74%
An online sharing platform (eg Strava)	40%

Source: National Cyber Security Centre, 'The Cyber Threat to Sports Organisations', July 2020

SP

This increasing reliance on digital technology makes sports organisations, much like those in the finance and digital health sectors, particularly susceptible to cyber attacks and ransomware. Such attacks can also prove to be costly. The NCSC report found that approximately 30 per cent of cyber attack incidents caused direct financial damage, averaging UK£10,000 per incident, while the biggest single loss was over UK£4 million. But despite the obvious threat, only 33 per cent of those surveyed in the report 'strongly agreed' that they had the right software and hardware in place to help protect the organisation from cyber attacks. 

**VIDEO**

Effectively combatting sports piracy

SportsPro Live 2020

**Watch now**

**Approximately 30% of cyber attack incidents in sports cause direct financial damage, averaging UK£10,000 per incident.**


SP

# Quantifying the value of content protection

**Typically, the content protection industry has struggled to prove the value of its services, largely due to difficulties in clearly demonstrating the link between content removal and prevented revenue loss. MUSO, a piracy monitoring firm which continuously tracks millions of devices and billions of web pages across 196 countries, has sought to change that by developing a methodology to measure and quantify the efficacy of content removals.**

According to the company, its data-driven approach 'is underpinned by the fact that not all illegally hosted content is equally popular. In other words, some content removals are more impactful than others, dependent on the scale of audience affected by the absence of the content.'

MUSO's methodology is built on three key metrics: a **removal impact score**, which differentiates between removals from high and low traffic sites; **visits disrupted**, which estimates the total number of piracy visits impacted by content removal; and **paid consumption gained**, which estimates the increase in paid consumption due to piracy content removals. Together, these metrics help paint a clearer picture of the effectiveness of content protection activity and seek to clearly show that investing in anti-piracy measures can deliver tangible ROI.

In live sports specifically, there is mounting evidence that content protection efforts work. In 2019, for example, UK broadcaster Sky Sports reported that viewership of its live Premier League coverage more than doubled across 17 matches after the league and its distribution partners successfully disrupted over 200,000 illegal streams the previous season. 



**ABOVE:** UK broadcaster Sky Sports has seen its Premier League viewership grow after stepping up its anti-piracy efforts

SP

## Targeting the 'converter cohort'

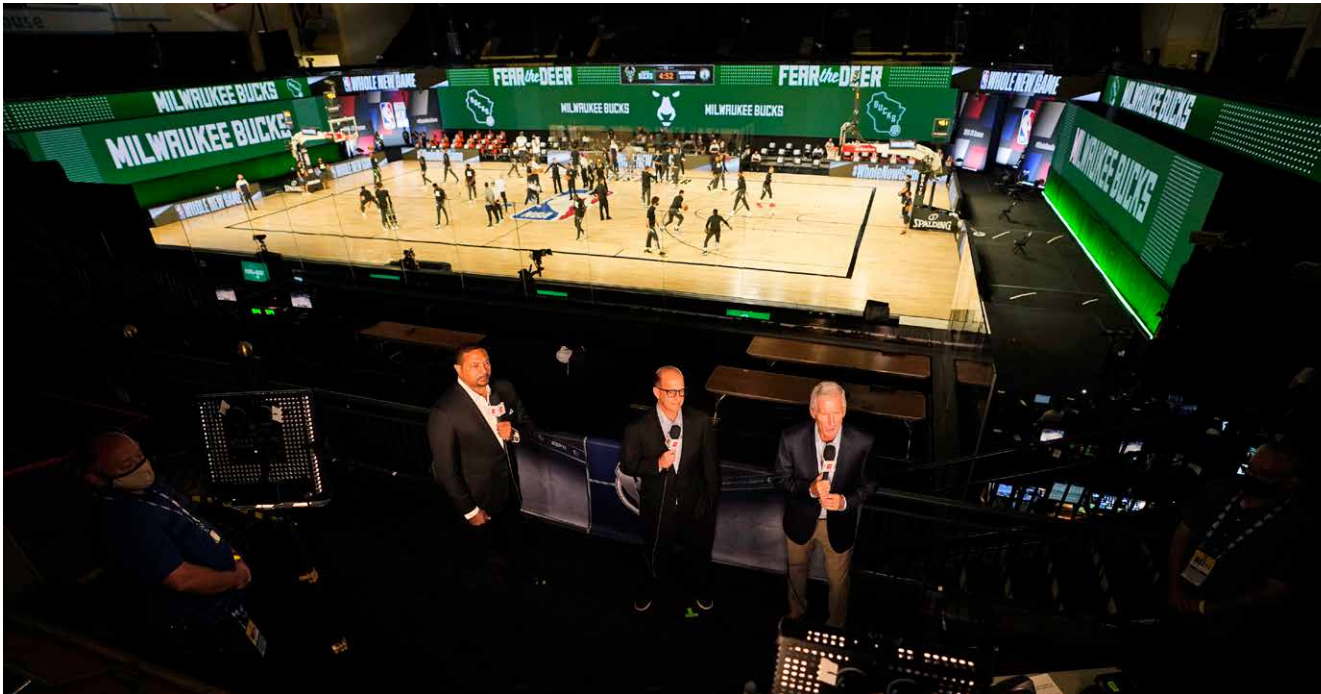
**Illegal streamers deemed most likely to switch to legitimate platforms have been dubbed the 'converter cohort'. A recent study by Ampere Analysis found that this group primarily comprises younger fans and are often families with young children, while it is also made up of avid sports viewers, many of whom watch ten or more different sports using connected devices.**

During the study, some 40 per cent of the converter cohort said they would subscribe to OTT sports streaming services, including single-sport platforms owned and operated by rights owners, with the balance opting for traditional pay-TV services, particularly those with exclusive coverage. Despite being the most likely to switch from illegal streaming, the study also found that 57 per cent of the converter cohort already pay for legitimate subscriptions, while 52 per cent are putting money in the pockets of illegal services.

Partly in response to this trend, several major sports leagues have adapted their broadcast distribution and monetisation models. ▶



SP



**“If you’ve got someone who’s looking for your content but not paying for it, well that’s an interesting target.”**

**LEFT:** The NBA has adapted its League Pass pricing options in part to monetise fans who might otherwise access illegal streams

The NBA is one prominent example. Having spent years watching its game content circulate social media platforms in real time, the league has sought to directly monetise its fanbase by introducing creative pricing options and microtransactions, including the ability for users to access a single fourth quarter for US\$1.99, on its League Pass digital offering.

“In one way it’s common sense; if you’ve

got someone who’s looking for your content but not paying for it, well that’s an interesting target,” says Andy Chatterley, MUSO’s chief executive. “What we’re always asked is: is there any value in a piracy audience? From a sports perspective, I think there’s two kinds of value.

“Firstly, there was this amazing research study from the University of Amsterdam a couple of years ago. They did a sample of

35,000 people across 13 countries in Europe and North America. What they discovered was that there’s very little difference between the levels of education or employment status - largely they’re the same person in terms of demographic - but their engagement is much higher. In fact, 95 per cent of illegal users also consume content legally, and their median legal consumption - how much they consume - is ▶

SP

typically twice that of legal users.

"We always think of piracy users as very high intent because they've gone to extra lengths, they've jumped through extra hoops, to find the stream online. And it's illegal. You can't dress it up; this is an illegal activity so they're risking prosecution and various different punishments in different jurisdictions to watch the sport that they want to watch.

"So you've got a high intent audience that if you can capture, if you can win their custom, are more likely to spend more with you in the long run. And that's really one of our key messages around the opportunity side of things."

One further consideration often overlooked in the piracy discussion is the indirect monetisation that can come through quantifying, if not converting, audiences who stream content illegally. In 2019, a study by MUSO and sponsorship valuation firm GumGum Sports - now known as Relo Metrics - found that clubs in English soccer's top flight are missing out on as much as UK£1 million (US\$1.2 million) in sponsorship revenue every fixture because of piracy. That study was based on an analysis of eight matches during the

2018/19 season, which on average drew an illegal audience of 7.1 million fans across 149 countries.

As Chatterley notes, failure to accurately measure and report these 'lost eyeballs' not only results in undervalued sponsorship deals, but also missed advertising revenue.

"You've got this audience that could be monetised from a sponsorship perspective, despite it being on unlicensed streaming sites," he says. "Commercially, that's a very interesting concept for sports in general. Broadcasters are not looking at this audience in the right way because they say, 'it's a piracy audience, there's no value'. They're also not necessarily selling the value on in terms of eyeballs.

"I think the problem comes from people's attitudes towards piracy audiences. They presume that they're of little value. All the data and all the studies that we see - literally all of them - point to it being the opposite.

"At some point you've got to turn it on its head. Are these the bigger fans? Are these the bigger eyeballs? Can we combine these two methods to get a real balanced and revenue-generating approach? For me, the answer is really in front of us." ● SP



**ABOVE:** Failure to accurately measure viewership could mean Premier League clubs are missing out on millions in sponsorship revenue



SP

## Further reading

['Pirates find the weak link and exploit it': Akamai's anti-content theft action plan](#)

[How to embrace the digital landscape for the next generation of sports](#)

[Showing the red card to streaming pirates? It pays to take a nuanced approach](#)

[Why combatting piracy requires a global approach](#)

[Why spoof-proofing your premium live sports content matters](#)

## Useful resources

**Verimatrix**

[Thwarting piracy in sports and esports](#)

**Intertrust**

[The new perspective on securing eSports](#)

**Intertrust**

[New challenges and solutions to protecting live-streamed video](#)

**Intertrust**

[Weighing Buy Versus Build Options for Securing Advanced OTT Video Services](#)

**Digital Element**

[Combat the Rise of OTT Sports Piracy with IP Intelligence](#)

**GeoGuard**

[A New Piracy Threat for Sports Leagues, OTTs & Rights Holders](#)

SP

# SportsPro REPORTS

For more information about future reports, please contact:

**Charlie Barker**

Global Partnerships Director

[cbarker@sportspromedia.com](mailto:cbarker@sportspromedia.com)

@SportsPro

[sportspromedia.com](http://sportspromedia.com)



## Verimatrix

Verimatrix helps power the modern connected world with security made for people. We protect digital content, applications, and devices with intuitive, people-centered and frictionless security. Leading brands turn to Verimatrix to secure everything from premium movies and live streaming sports, to sensitive financial and healthcare data, to mission-critical mobile applications.

Find out more at [verimatrix.com](http://verimatrix.com).



## Intertrust ExpressPlay

Intertrust ExpressPlay offers robust protection services for distributors of live and VOD content, enhanced by a rich partner ecosystem. The cloud based ExpressPlay Media Security Suite features the ExpressPlay multi-DRM service, ExpressPlay XCA broadcast security solution, and ExpressPlay Anti-Piracy services, with proven scalability in the largest OTT streaming platforms globally. Find out more at [expressplay.com](http://expressplay.com).