

Inside the World of Video Pirates

How Do We Stop Them?

Downloading...

Critical Data



Table of Contents

The History of Video Piracy	1
Do We Need to Solve the Internet Video Piracy Problem?	2
How Does the Piracy Industry Work?	7
Can We Stop Them?	13
360° Posture	15
Conclusion	20

Inside the World of Video Pirates

The History of Video Piracy

Video piracy is not a new issue. Since the dawn of professional movie production, there have been people willing to make a fast buck by exploiting “private property in the form of copyright infringement”. During the silent movie period, the concept of “bicycling” (extended screening of movies in theatres) became so popular, Hollywood would send out “checkers” to catch unscrupulous theatre owners in the act. Then came the “dupers”, who would make copies of movies using positive prints to create new negatives. As technology developed, “cam rips” (bootleg cam recordings) became a popular choice for copyright theft in the ‘60s, with the industry calling them “video of indeterminate origin”. But it wasn’t really until the ‘80s, with the advent of VHS, that pirating actually became a lucrative business that could be scaled. For those growing up in this period, who could forget that a purchase from the ice cream van or corner shop would often end up with you walking away with a clutch of the latest movie titles (albeit of very poor quality) along with your Cornetto?

In the ‘80s and ‘90s, along with physical formats of pirated content such as DVDs that required relatively little technical expertise, piracy started to get more complicated. First, pirates started to go online with the advent of better internet connectivity. The warez scene, or “the scene”, (which originally was associated with illegally distributing video games but morphed into other forms of piracy) developed what has been described as the first true internet subculture. Whilst it would be trite to suggest that warez groups are singularly responsible for the growth of piracy, they did (and still do) play an important role in the origination and distribution of content.

Equally, with the growth of pay TV in the ‘80s and ‘90s, we witnessed new forms of piracy such as illegal access to encrypted transmissions. This encouraged the rapid development of conditional access technologies, but also – because of the potential commercial gains and technical complexity – pirates started to become more sophisticated, organized, and business-minded.

During this period, “sharing” over the internet was also made easier by new players that encouraged unauthorised file movement; Napster was the genesis of this concept. In spite of its demise in 2001, peer-to-peer (P2P) file-sharing sites started to appear across the internet, making digital distribution by far the easiest and most effective way of distributing thousands of pirated video copies to many millions of viewers instantly. The new generation of sharing platforms were technically more refined, and protocols such as Morpheus, Gnutella, LimeWire, eMule, and BitTorrent prospered. The platforms and protocols generally did not store copyright-protected content on a central server but facilitated direct P2P exchanges among users (peers) to avoid liability and vulnerability.



The warez scene, or “the scene”, has been described as the first true internet subculture.

As legitimate digital video technology has developed to deliver better experiences to viewers over the internet, so too have the pirates. The pirates of today now use a range of attack vectors to retrieve and distribute content. Re-streaming of linear channels is capable of providing an experience indistinguishable from TV. Cyberlockers – such as Megaupload (succeeded by Mega) – make use of cloud storage hosted at locations that aim to be out of reach of copyright enforcement. The means of distribution are varied and robust, such as streaming devices or websites. Pirate businesses offer their customers easy user experience, customer service, and a range of flexible business models. One interviewee for this paper suggested that legitimate video streaming businesses could learn a great deal from the pirates!

With this backdrop in mind, this paper will explore the “IP piracy challenge” and ask the question: Can it ever be stopped?

Do We Need to Solve the Internet Video Piracy Problem?

Before we examine whether piracy can be stopped, we must first understand if the problem actually warrants attention, which might sound slightly counterintuitive in a white paper examining piracy. The TV and film industries are weathering an era of technical and commercial upheaval. Broadcasters and film distributors have many competing demands for OpEx and CapEx to support production, new technical formats, and in many cases, new business models. As such, funds required to fight piracy will be prioritised along with other demands in the business, so we need to be clear about the relative value and potential return on investment.

The industry historically invested approximately 1% of licensing costs on anti-piracy measures, but this has declined over the years as conditional access technologies stabilised and became effective at preventing pay TV fraud. IP-based piracy is not new, but in their paper on piracy risks, Parks Associates describes the media industry as being in an early adopter stage. They suggest that most efforts to date have not been focused on preventing theft or redistribution, but have been more focused on credential stuffing. As the video market transitions towards an all “IP” future and pirates are able to exploit new forms of distribution, is this something we need to re-address? To answer this question, we need a clear understanding of the problem. What is the true extent of piracy globally and across different regions, and what are the business impacts?

The extent of the problem

There are many outstanding studies on the topic of video piracy, but it’s still difficult to establish the true extent of piracy globally, regionally, and nationally. The simple reason for this is the absence of a consistent method to track the problem. As such, the breadth of narrative can be confusing to any media executive looking to establish priorities.

Data sets provided by commercial organisations are useful but can often be at odds with one another based on methodology. Noncommercial studies, whilst thorough, are generally limited to specific countries or groups of countries because of cost or regulatory boundaries. Terminology used in reports has not been standardised, leaving readers confused. Finally, absolute figures are hard to define, as many viewers of pirated material are also avid users of legitimate services.

Piracy, in the words of one interviewee for this paper, is like playing a game of whack-a-mole. Everyone understands the generic attack vectors and forms of distribution, but no one really understands how prevalent each of these are – especially the form of original theft.

More recently, however, there have been several studies that have started to use repeatable methodologies to quantify the extent of piracy. As an example, the European Intellectual Property Office (EUIPO) conducted a study into the impact of piracy across member states. They were able to estimate that 13.7 million people across EU countries are accessing illegal pirate services of differing flavors. They were able to identify that the Netherlands, Sweden, and Spain have the highest percentages of offending viewers within their populations, with 8.9%, 8.5%, and 6.9% respectively (the EU average is 3.6%). The United Kingdom (2.4 million), France (2.3 million), and Spain (2.2 million) have the largest populations using illegal services regularly. (Note, as an example of research discrepancy into piracy adoption, a recent YouGov study identified that there were 4.9 million illegal Kodi boxes in operation throughout the United Kingdom.) In Europe, unlike other regions, there has been some decline in piracy. Whilst the actual figures are debated, this is a direct result of the apprehension and prosecution of pirates, plus the renewed effort of some governments to educate their population on the damages that piracy brings.

13.7 Million
Estimated number of people in the European Union who access pirate video.

In North America, the picture is less clear. Sandvine analysed the usage of multiple fixed line “tier 1” networks and estimated that 6.5% of households were regularly communicating with pirate sites. In contrast, a Park Associates report identified that more than 14.1 million U.S. households accessed pirate video in 2019, putting the figure at approximately 16% of the total pay TV market. Whilst these are comparative figures with the European Union, methodology differences may underestimate the challenge in that region.

The picture in Asia Pacific is much more complex. Being a diverse region with no unifying regulatory body, most studies are conducted within specific countries, and typically through commercial or industry bodies. The available research, however, shows that the region has some of the most voracious viewers of pirated material.

The 2017 study by the University of Amsterdam identified the piracy habits across Hong Kong, Indonesia, Japan, and Thailand. Results showed that both the Indonesian and Thai populations demonstrated a very high propensity to pirate content, with the study estimating between 65% and 54% of their internet populations, respectively. Hong Kong registered 27% of their internet population; Japan registered a mere 12% of their internet population (11% of the total population).

An independent consumer survey report commissioned by the Asia Video Industry Association in 2019 corroborated these results and found that in Hong Kong, 24% of consumers use internet streaming devices to access pirated channels. This increased to 28% of consumers in the Philippines, 34% in Taiwan, and 45% in Thailand.

From these figures, we can see that video piracy – and in particular, TV piracy – is still a serious issue globally. That said, we still need to evaluate the impact of piracy to ascertain whether further time and resources should be invested in tackling the problem.

What is the impact of piracy?

One area that has been researched and described extensively is the impact of video piracy to the long-term sustainability of the media business model. Most commentators agree on the strategic challenges, but there is considerable variance on absolute figures. This becomes an important factor when considering the relative value of investing in anti-piracy initiatives versus other business demands. There are many factors that could be considered when examining the impact of piracy, such as the spread of malware and other malicious cyberthreats; however, for the purposes of this paper, we have focused on three key areas of impact: financial, jobs, and licensing.

Financial impact of piracy

Negative financial impact due to video piracy is generally acknowledged by most commentators. Studies have estimated losses to the industry as high as \$52 billion by 2022 globally (Digital TV Research 2017), with GDP loss estimates due to a reduction in taxes at even higher levels. In the United States alone, GDP losses due to piracy have been estimated to be between \$47 billion and \$115 billion (Blackburn et al, 2019).

Despite eye-watering figures – by any stretch of the imagination – many distributors still see the prevention of piracy as a cost to their business rather than a positive revenue driver. The reasons for this are complex, but sound. First, it is hard to prove that the prevention of piracy would lead to additional revenue. Indeed, research has pointed towards piracy sometimes improving subscription revenues (Sanchez, 2012), as it provides free advertising for legitimate services. The “sampling effect” has also been described as a way of introducing viewers to new actors or genres, which in a paid business model might never be achieved (clearly this is nuanced by genre and the availability of legal alternatives). Studies have shown that people who consume content from illegal sources are also the video industry’s largest customers, i.e., people who are interested in films or TV series tend to consume more via any available channel. As such, you cannot compare the legal and illegal consumption of individuals and conclude that any correlation with financial loss is causal.

In the same vein, “credential sharing”, whilst seen as a form of piracy, is often overlooked by subscription video on demand (SVOD) services, as again it provides marketing benefits. In the words of one CTO, “We know it’s occurring, but we also know they’ll return eventually, so right now it’s not high on our agenda”.

The second challenge when reviewing financial losses is that researchers often use the “multiplier effect”, which can in turn incorrectly overestimate the financial impact to the industry. As an example, the Motion Picture Association of America (MPAA) admitted that financial losses due to piracy communicated in one of their reports overstated the problem significantly (Greenburg, 2015; Sanchez, 2012).

The financial impacts of video piracy are therefore highly nuanced regionally, nationally, and per company. A 2017 study by the University of Amsterdam identified the complexity of understanding the financial impact of piracy on a global basis. It identified that individual national attitudes continue to have an overriding impact on piracy adoption, showing examples across both developed and developing countries where copyright legislation was present. This confusion clearly seeds doubt in the minds of TV and studio executives, certainly when considering budget prioritisation.

That said, the substitutional impact (i.e., when a viewer refrains from buying or watching specific content legally after having acquired or consumed it from an illegal source or displacing legal consumption via competition for people’s time) is recognised as a serious challenge for the industry. A study commissioned by the U.S. Chamber of Commerce published in 2019 estimated that total global revenue losses in 2017 from digital video piracy based on displacement and other factors were between \$40.0 billion and \$97.1 billion for the film industry and between \$39.3 billion and \$95.4 billion for the TV industry. In the United States, these figures were calculated as \$2.5 billion (film) and \$3.6 billion (TV), illustrating that piracy is actually more of a global issue.

\$79.3 – 192.5B
Estimated cost of global piracy to film and television industries.

Whatever the view on financial losses through displacement, we can be clearer on the financial gains made by pirates. Within the European Union, it is estimated that pirates generate more than €941.7 million in annual revenues through paid subscriptions and advertising. The United Kingdom, France, Germany, the Netherlands, and Spain generate nearly 76% of those revenues (EUIPO 2019). In the United States, Sandvine estimated that the piracy ecosystem generates a similar figure, with revenues in excess of \$1 billion. No viable studies have been conducted across the Asia Pacific or South American regions to provide a comparative figure.

Impact of video piracy on jobs

Whilst most narratives concerning the impact of piracy focus on revenue loss, the TV and film industries support millions of jobs, from set designers, makeup artists, and musicians to producers and directors – and piracy is putting these at risk. Until recently, the link between video piracy and job losses has been largely based on several high-profile announcements of services downscaling or shutting down. Examples include beIN announcing 300 job losses as a direct result of piracy, and RTL International announcing the cessation of their international pay TV channels. Another notable example is the cancellation of the psychological horror-thriller *Hannibal*, due to “poor ratings”. The series, however, was ranked as the fifth-most illegally downloaded show in 2013. “Disappointed fans of the show can only look to themselves and peers to blame”, according to its producer, Martha De Laurentiis, who said “Hannibal’s cancellation had a lot to do with piracy”.

With the advent of more-considered studies, we are now starting to understand the wider impact. In their report on the impact of digital piracy on the U.S. economy, Blackburn, Eisenach, and Harrison estimated that between 230,000 and 560,000 jobs were lost in the United States in 2017 as a direct result of pirating activity. The employment losses were attributed across all areas of the industry, including both direct and indirect roles, creative and noncreative.

Fewer equivalent studies have been conducted into the impact on job losses outside of the United States due to unequal distribution of roles across different countries – unlike the United States, which is a homogenous market. Research from the Federation for the Protection of Audiovisual and Multimedia Content (FAPAV) in Italy, however, estimated that direct job losses at risk because of piracy totalled almost 6,000. Again, this was based on the wider impact on roles associated with media production and distribution. Looking at the methodologies used by FAPAV, it is easy to see how job losses across other EU member states could easily be in line with those identified in Italy. Moreover, in the larger content-producing/exporting countries such as the United Kingdom, Spain, and Germany, these could be even higher.

It must be noted that the extent to which piracy impacts employment has been refuted by a number of researchers. Several experts have called into question the validity of “displacement” or the true impact of piracy on derived industry revenues, which in turn impacts employment. Several researchers have suggested that the measurement of “opportunity” displacement might be a more accurate metric when reviewing job losses. This is because of the reliance on freelance creative professionals within production who may not be fully employed if piracy impacts programming investment. It has also been noted that the current buoyancy in the production sector, driven in part by investment being made by SVOD services, reduces negative employment prospects due to piracy.

Despite the ongoing debate regarding the levels of piracy displacement, it’s clear that copyright infringement has a dampening effect on employment, or certainly employment opportunity. Any industry that experiences product theft at such prodigious levels would struggle to maintain full employment. The impact will likely be more pronounced in countries or organisations that have a strong production slant or operate international channels.

Impact of video piracy on licensing

We’re beginning to see signs that piracy is impacting licensing, which is the lifeblood of the creative industry, and arguably a more damaging strategic issue than any other. Put simply, why would potential distributors pay significant sums of money for rights when content is readily found for free through pirate sites? Conversely, why would rights owners sell to a leaky distributor who has the potential of damaging their international sales?

As a genre, sport is certainly susceptible to this, with recent press releases illustrating the point. Yousef Al-Obadly, the chief executive of beIN – one of the largest sports rights buyers in the world – stated that “the sports rights bubble is about to burst because of global piracy”. He was signaling that the value of rights to his organisation will be based on the level of exclusivity. If content being acquired is not exclusive because of piracy, then its value diminishes significantly.

In another article, Oscar-nominated, Emmy award-winning producer Jason Blum described how piracy is having a direct impact on the funds being made available for the innovative, risky movies that push the boundaries of storytelling. He suggests that at some point in the not-too-distant future, the numbers will become unsustainable and the studios will have to cut back their slates. "They will not cut back on their franchises (where they make their real money) or low-budget horror movies, they will cut back on the art movies that are risky and do not have an easy path to profitability. Pretty soon, there won't be movies like *The Big Short* to even steal".

“ *The sports rights bubble is about to burst because of global piracy*”.

– *Yousef Al-Obaidly, CEO, beIN*

And so, to answer the question, do we need to solve piracy? At an initial glance, the return when implementing anti-piracy strategies for most distributors seems clear – the protection of core revenues, exclusive rights, and jobs. Piracy is prevalent in all regions, and despite some limited success in the European Union, is set to grow over the next few years. It is clear that piracy has a detrimental impact on the finances of producers, rights owners, and distributors alike. What is unclear, however, is the extent of these impacts at an organisational level, making it notoriously difficult for any board to justify anti-piracy investments.

This is a highly nuanced subject, and dependent on a range of factors – including whether pay TV or free-to-air is the dominant form of viewing within a nation, whether a business is a net exporter of rights or an importer of exclusive rights, and whether a business has a competitive advantage within a particular genre such as TV dramas or movies. Once these factors are understood, it is then possible to create a clear financial risk analysis at an organisational level, which in turn can help inform an appropriate strategy.

What is common across media companies, irrespective of business model, are the more strategic challenges created by piracy – namely, the impact on employment opportunities and licensing. These are both fundamental to the health and long-term sustainability of the industry, especially with deficit funding for production now commonplace. Moving forward, therefore, we expect to see premium rights owners, industry bodies, and even regulators insist that companies across the ecosystem start to implement more comprehensive strategies to tackle the issue. We will explore these in the final section of this paper.

How Does the Piracy Industry Work?

As in any battle, it's important to understand your adversaries, so you can fathom their motivations, tactics, strengths, and weaknesses. Unlike many other aspects of video piracy, there are very few reliable studies in this area, probably for obvious reasons.

Who are the pirates?

Studies often describe video pirates as a nefarious homogenous group with a common purpose: to make money. A cursory internet search will bring up numerous articles describing how police have swooped in on a particular "pirate gang" who were generating millions of pounds in revenue from their site.

These descriptions conjure the image of pirates as organized, opportunist criminals running complex, sophisticated businesses, and this is certainly true in many circumstances. Like so many aspects of the web, however, digital piracy is by its nature global and anonymous. It's difficult to track with certainty where a pirated movie or TV show originally came from, or who pirated it. What we do know, however, is that there is a complex array of groups and subgroups, each with their own drivers, levels of sophistication, and inter-group reliances.

The release groups

Several studies on pirates describe an altruistic persona, reminiscent of the original warez scene. Members often see themselves as “romanticised” revolutionaries in a struggle against big corporations. Those who are caught and prosecuted are often lauded as heroes. Pirate Bay cofounder Fredrik Neij remarked after completing his 10-month prison sentence, “It was well worth doing prison time, when you consider how much the site means to people.”

In this group, a sense of community binds the pirates together – albeit with a misplaced sense of altruism – but they are certainly not necessarily driven by profits. Membership to sites where content is uploaded is earned by those who are worthy and trusted. Different groups and individuals specialise in certain genres and compete to acquire new material, which is then rewarded with recognition. Content that is of bad quality or infected with viruses is “nuked” and the uploader is discredited within the community. In his *Vanity Fair* article on the growth of torrenting, Steve Daly characterised release group members as classic computer-geek stereotypes: socially awkward, obsessive by nature, and people for whom stealing content provides a sense of belonging. FACT described the structure very differently: “These are complex, sophisticated, and well-organised hacker-style groups who are suspected of being involved in other kinds of cybercrime, like spreading ransomware or hacking people’s bank details to sell on the dark web”. Whatever their motivation, and as with the warez scene, the groups have a clear hierarchy and structure with many written laws and strong trust-based ties.

The site operators

The publicly accessible sites, such as cyberlockers or streaming sites, are managed by another distinct group – the site operators. It's not known if the release groups and site operators are the same individuals, but many studies have made the case that there is a significant overlap and reliance between the two. Come what may, the site operators certainly make money out of the process. Site operators often run several “mirrors” – sites that duplicate each other so that if one is taken down by the authorities, they can still stay online and make money. As with any sophisticated retail operation, there are also site wholesalers, e.g., Streamango and Openload, which between them fed more than 50 of the top illegal video streaming and linking sites. The most brazen brand, however, has to be beoutQ – which, despite having its illegal feeds over Arabsat curtailed, continues to distribute content over the internet in what has been described as piracy at an industrial scale. Whilst it's easy to see how release groups may not necessarily be motivated by financial gain, site operators certainly are. In some cases, there is a basic need to cover site costs (as was suggested by Pirate Bay founders). For others, the potential profits are too lucrative, and the site operators have developed to become highly sophisticated global businesses.

The internet streaming device wholesalers

Another distinct video pirate persona is the internet streaming device wholesaler. The growth of these devices – in particular those that utilise Kodi – provides a relatively steady and predictable revenue stream for opportunist criminals, capable of generating hundreds of thousands of pounds a year.

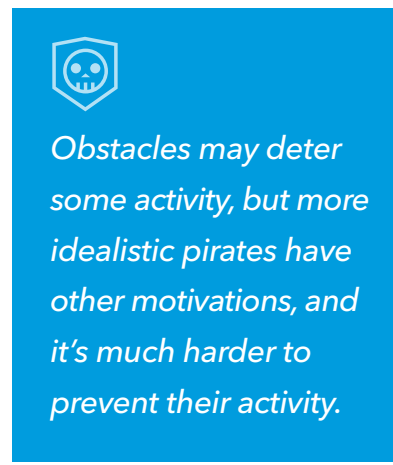
Wholesalers often import the boxes through entirely legal channels and modify them with illegal software at home. Others work with sophisticated criminal networks to import boxes and then sell them online, sometimes managing to sell hundreds or thousands of boxes before being caught. The availability of illegal add-ons to Kodi software has helped the organised gangs to reach a wider audience. While Kodi itself is legal, the add-ons are not; they have no parental controls or security standards, and open users to a range of risks from adult and inappropriate content.

The amateur pirate

More recently, and coupled with improvements in livestreaming over social media platforms, we've seen a new persona emerge – the amateur pirate. Unlike the site operators, illicit streaming device (ISD) wholesalers, and release groups who are driven by profit or organized altruism, people in this group are less aware or ambivalent to the fact that piracy is illegal, and are responding to either the cost of certain content genres, subscription fatigue, or the ubiquity of social media. To illustrate, the Mayweather-McGregor boxing match recorded 132 million pirated views from more than 6,977 illegal streams. Many of the stream originators were simply people holding their phones in front of their TV screens and using social media platforms to deliver the content.

The distinctions between the pirate groups are important to understand. As with any organised criminal activity, gangs looking for profit seek easy targets to maximise their returns. Obstacles placed in their way, however rudimentary, may deter activity. More idealistic pirates are driven by other motivations, and as such it is much harder to prevent their activity.

What is true in almost all cases, however, is the presence of an ecosystem of organised participants consisting of primary infringers (providers of unauthorised content); a series of passive and active intermediaries; facilitators and enablers who, for example, help consumers implement middleware; and finally, the viewers of pirated material themselves, which we will turn to in the "Who watches pirated content?" section.



Obstacles may deter some activity, but more idealistic pirates have other motivations, and it's much harder to prevent their activity.

How do the pirates acquire content?

Because of the ubiquity of digital workflows, there are now many viable methods for pirates to steal content, but for obvious reasons there is very little reliable analysis into which methods are favored or most prevalent for the different subgroups. What information is available, however, demonstrates a range of weaknesses across the entire value chain that can be exploited. For ease of illustration, we can group the attack vectors based on use case.

Inside the World of Video Pirates

Simulcast of TV channels and live events. One of the fastest-growing forms of piracy is the capture and redistribution of TV channels or live events. Indeed, in the 2019 Asia Video Industry Report, the Coalition Against Piracy identified that many viewers who had switched to ISDs had also cancelled legitimate subscription services, making ISDs their main TV viewing service. As an example, in Hong Kong, nearly one in four households use ISDs, and of these, 10% have cancelled their subscription to legal services. Additionally, the prevalence of smartphones – coupled with improvements in livestreaming across social media platforms – now permits somebody to simply point a device at a TV screen and stream content. Pirates therefore use a variety of methods to capture live channels, including:

- Tampering with video playback software or Android OS
- Recording screens during playback or capturing during a screen-share session
- Intercepting decrypted video using HDCP strippers connected to set-top boxes
- Using credential stuffing attacks to access and use legitimate viewer details
- Tampering with video to defeat watermarking, such as re-quantisation
- Transporting video out of a given market using a VPN

On-demand content. This is arguably the most prolific form of piracy globally. Release groups, in particular, prize new video assets and seek to capture prerelease TV shows and movies before they've been aired. Interestingly, in this scenario, the structure of the creative industry itself presents a range of opportunities for pirates. The fact that so many different organisations and freelance staff are involved in the production and post-production processes provides pirates with many opportunities to identify and exploit vulnerabilities. Indeed, one individual interviewed for this paper illustrated the point by describing how pirates have targeted internet-connected editing tools and associated storage platforms to access new shows before they reach playlist. Other methods used by pirates to acquire video assets include:

- Data-centre breaches, which have resulted in the theft of user credentials, cryptographic keys, or video content
- User identification theft from freelance and full-time staff providing access to video through various systems
- Recordings of physical assets (less prevalent now) for sharing and distribution
- System hacks against various production systems providing direct access to video assets
- Ripping content from legitimate sources, e.g., iTunes
- Cinema filming systems
- Direct theft using man-in-the-middle attacks

On-demand content is arguably the most prolific form of piracy globally.

How do pirates distribute content?

Unlike methods of content acquisition, this area of the pirating business model is well-documented, and as is the case with legitimate streaming, pirates use every possible channel and technical innovation available, including:

- Custom-built IP set-top boxes that access preprogrammed TV streams
- Software running on PCs and streaming devices that enable pirate distribution, e.g., Kodi
- Apps that are side-loaded onto popular retail streaming devices
- Websites and social media services that host user-created content, such as YouTube
- Websites that stream content to viewers with links that can be discovered via internet search or promoted over social media
- The ever-present download, file hosting, cyberlocker, and torrent sites

Whilst the distribution strategies of the various pirate groups are less understood, we can see that release groups would possibly favour asset-sharing models, such as cyberlockers and torrent sites, because of the inherent support for ubiquity. As a contrast, the financially motivated pirates would favour the ISD/streaming strategy to emulate legitimate services and the ability to encourage multiple revenue models. It must be noted that the relationship between the pirating groups is less clear. Do the site owners rely on the release groups for on-demand assets? Are the site owners self-reliant, or do they employ more technically proficient groups to defeat anti-piracy technologies?

One common facet in most cases, however, is the need to generate revenue, at the very least to support basic infrastructure costs. Most sites have ad-based revenue models, but certainly sites that support simulcast streaming have adopted a multifaceted approach, including subscription or hybrid models.

It was reported by TechCrunch (2008) that Pirate Bay was generating more than \$4 million in ad-based revenues per annum across its 2.5 million subscriber base. FACT also identified in their 2017 report that even smaller sites could generate ad revenues of \$100,000 per annum. Whilst these figures are small in comparison with legitimate businesses, pirate profit margins are estimated to be as high as 80-94% (FACT 2017). When these are then compared with a legitimate business with 7-20% margins, you can understand the attraction.

Ads are typically banner ads or pop-up windows for casinos, dating sites, pornography, and download services. But some feature ads that have been placed using programmatic technology, which means legitimate brands often don't know exactly where their ads are going but can give the site an impression of respectability. In subscription-based models, pirates encourage users to sign up for a "premium" account, featuring an improved viewing experience and no advertising, in return for a monthly payment. Prices vary from site to site, and most will offer a range of packages with different options and costs. But typically, subscriptions will cost from £5 up to £50 per month.

There is a darker side, however. Uploaders into the torrent sites make little or no money – and as competition intensifies between pirates, many streaming sites have resorted to the use of malware, viruses, adware, or spamware. Malware is often designed to promote piracy, identify theft, forced cryptocurrency mining, and illicit online material, such as pornography. The individuals who distribute malware are sometimes well-compensated for their efforts. A study in the United States found that one in every three pirate sites exposed users to malware, with criminal gangs making at least \$70 million a year by charging hackers to embed malware (Digital Citizens Alliance 2017).

More recently, pirates have been exploring new ways to make money, including “content ransom” attempts. In this scenario, hackers steal (or claim to have stolen) TV episodes or films and subsequently demand ransom payments from the commissioning body. Several of these have been publicised, including the 2017 thefts of the TV series *Orange Is the New Black* and the movie *Pirates of the Caribbean: Dead Men Tell No Tales*. HBO experienced a cyberattack in which 1.5 terabytes of data was believed to be stolen, with hackers threatening to leak episodes and scripts of *Game of Thrones* (Sulleyman 2017).

Livestreaming of major events or sports has been particularly targeted by pirates because of the costs involved for fans to access legitimate feeds and the events' emotive appeal. In some circumstances – for example, high-profile football matches – records show higher numbers of pirated streams than legitimate (Forbes 2015).

Who watches pirated content?

There have been numerous studies into why normally law-abiding people watch pirated video. These include financial justification, ignorance, and the basic ability to access content without windowing restrictions. Suffice to say, however, that anyone with internet access can visit a rogue site or use a perfectly legal device and stream all sorts of high-quality content using viewer-friendly business models. Indeed, pirated content through Kodi boxes was once described as the most successful digital rollout in British TV history! Motivations differ significantly across the viewer population, and again, it's useful to understand these drivers in order to combat the problem.

In their study on the consumption of pirated material, VFT identified a range of personas and their drivers, which are summarised below.

- a) The “Content Anarchist” believes in communal and unfettered access to online content, and that any charge of any type is unacceptable. The Content Anarchist fundamentally does not believe that piracy is illegal.
- b) The “Content Robin Hood” is less extreme in their views and open to consider alternative legitimate propositions. This group is loyal to the tenets of sharing content, and as such, vested in populating and disseminating files.



For high-profile football matches, records show higher numbers of pirated streams than legitimate.

- c) The “Utilitarian” justifies their actions based on the belief that content is of little value. They will only purchase content that has a lasting value and can be watched repetitively. They understand that piracy is illegal, but nonetheless continue.
- d) The “Lazy” viewer is influenced mainly by cost savings and availability of titles, and is often either unaware or ignorant to the fact that piracy is illegal. In its study, VFT suggests that the Lazy and Utilitarian personas represent up to 70% of the total viewing community – and accordingly, efforts to educate, convert, or penalize those groups will have the greatest impact on piracy.

Can We Stop Them?

The unfortunate short answer to this question is: not entirely. The history of piracy has shown that, as long as content is being created, there will always be pirates looking to exploit the relationship between supply and demand. All is not lost, however. What is clear from various piracy initiatives across the world is that if the challenge is tackled strategically, then it can certainly be minimised. Every organisation involved in the value chain, from production to distribution, legislators, and regulators, has a role to play.

Demand-side initiatives

Provide access to content. Data has consistently shown that viewers of pirated material are often the biggest purchasers of legitimate content. As such, there is a strong correlation between providing viewers with content that they want to watch (with a good streaming experience at a reasonable price) and a reduction in piracy. A new study delivered by the Vocus group in New Zealand found that whilst 11% of viewers obtained copyrighted content via illegal streams, 55% of these would obtain the same content through legitimate streaming services if made available. In another example, after Sweden introduced strict anti-piracy laws, it remained broadly unaffected – piracy rates of TV actually increased after the law, only decreasing years later, following Netflix’s entry to the market.

Unfortunately, the legal maze and costs associated with global rights is a complicated subject. But suffice to say, ubiquitous access to content will not happen anytime soon. That said, until relatively recently, many over-the-top (OTT) services provided by broadcasters or studios were a defensive play, and not necessarily seen as a significant value generator. As such, video assets were either hidden behind expensive OTT paywalls or not made available at all. Times have changed, and with the success of the global SVOD players, many primary rights owners are now investing heavily in their online services. As these services roll out globally, we should expect to see a decrease in piracy.

Education. For those who work in the industry, understanding that piracy is a criminal activity in the same vein as any theft is obvious; to those outside it, it is anything but. Piracy to the wider population has become something that “everyone” does, and therefore no longer appears illegal because the behavior is normalised. Disappointingly, the impact of piracy education on the general public has been limited, but efforts should continue to remind people that piracy is a crime and has a real impact on livelihoods. Likewise, advertisers should continue to be educated on the impact of brand association with pirate sites.

Legal. Many commentators have highlighted the ineffectiveness of legal action as a means of curbing demand. Aside from the logistical challenges of bringing action against thousands or millions of individuals, there are considerable technical hurdles in associating IP addresses, especially with the growth of cyberlockers. Moreover, with data protection laws becoming more established, legal precedent is denying the link between IP addresses and individual identities (legal precedent has denied the link between IP addresses and copyright infringers in the U.S. states of Washington, Florida, California, and recently in the U.S. Ninth Circuit Court of Appeals). There are several innovative cases underway that may provide alternative measures to prosecute repeat viewers of pirated material, but legal activity may be better directed towards the acquirers and pirate site owners.

Supply-side initiatives

Data. One glaringly obvious requirement is the need to establish a standard methodology to measure the extent and impact of piracy across the global markets. During the process of researching this paper, it became clear that a significant portion of confusion surrounding piracy lies in the plethora of studies available. This does not allow for any form of continual or contextual analysis and introduces confusion for governments and distributors alike when prioritising activity. This could be easily remedied through industry bodies such as the Alliance for Creativity and Entertainment (ACE), the MPAA, or regional bodies such as the EUIPO taking a leadership role.

Legal and Regulatory. Unlike the demand side, we are seeing several excellent initiatives in this space at both a national and global level. At a strategic level, various industry bodies such as ACE, or governmental initiatives such as FAPAV in Italy, are starting to see a concerted effort to identify and prosecute video pirates and tighten the legislative loopholes around the world. These efforts require coordination and access to relevant data.

Technical and Operational. In the same way that we want to make it easy for viewers to access great entertainment through legal channels, we want to make it hard for the pirates. What that means in practice in today's digital world is organisations reviewing operations and identifying weak areas in their workflow, from production to distribution, and applying appropriate measures. Many rights owners (certainly film and premium sports rights) already stipulate minimum acceptable operational standards for third parties. These are sometimes contractually binding – however, because of the cost and complexity involved, rights owners may only stipulate the bare minimum of protection. As an example, the MPA best practice guidelines for handling valuable content are comprehensive, but voluntary. No single organisation can solve the piracy challenge, and if there are weak links in the chain, the issue will never be eradicated. Taking a 360° approach towards piracy, and implementing relevant procedures based on roles within the workflow, will help significantly.



No single organisation can solve the piracy challenge, and if there are weak links in the chain, the issue will never be eradicated.

Cooperation. It's clear that improved cooperation is needed to provide rights owners, distributors, and legislators with the insight and operational coordination to fight pirate activity. Whilst the TV and film ecosystems are used to competing, the potential impact of piracy is too significant for cooperation to not occur. This needs to take place at all levels of the industry and at all steps of the process, from production and on-set content security through to transmission. The more companies and organisations that are involved, the more effective the overall solution. Unfortunately, the reverse is also true. If there are weak spots, that weakness is there to be exploited.

360° Posture

After reviewing the means by which the various pirate groups acquire and distribute video, we have constructed a framework through which customers can strategically review their threat landscape and evaluate relevant technical solutions. At Akamai, we develop services to form a strategic anti-piracy posture encompassing three core facets: Protect, Detect, and Enforce. These in turn can be combined with other activities to form an effective anti-piracy framework.

Protect

1. Protect against credential stuffing. As described previously in this document, credential stuffing is a popular attack vector used by pirates to acquire viewer details. The primary means for pirates to execute a credential stuffing attack is through automated bots on login pages. Akamai has worked with media companies large and small to tackle this challenge, and that work has yielded many best practices. Here are our top recommendations:

- a) Code login pages/API with OWASP. Write secure code according to the OWASP best practices and do a penetration test on your login endpoints.
- b) Use anti-DDoS protection. This can help you prevent volumetric botnets from reaching your infrastructure and overwhelming your assets.
- c) Utilise a bot management solution. This can help you prevent sophisticated credential abuse attacks by verifying user behavior and device telemetry.

2. Protect against theft from systems. Theft from internal production systems, digital storage, or the public cloud is rarely communicated by the industry, but as we identified, it is an important source of pirated material. Broadly speaking, we see several forms of video asset theft:

- a) Direct hacking or man-in-the-middle attacks by pirates
- b) Theft by employees or freelancers
- c) Capture of unique system ID, such as passwords

There are multiple technologies that companies involved in the production and pre-distribution workflow can employ to minimize the risk, but essentially, they revolve around the concept of Zero Trust. In an industry that has historically operated through high levels of trust within its ecosystem, this may sound draconian. The reality, however, is that in a digital world the norms and sanctions that have held the media community together no longer exist.

Zero Trust is a framework that companies are using to transform their core IT and media production systems and replace more traditional perimeter-based security systems. It is built around the idea that there is no longer an internal network where anyone or anything can be trusted. Core components of Zero Trust framework include: securing access to all resources, regardless of location or hosting model; enforcing a strategy of strict access control, based on least privilege; and inspecting and logging all traffic for suspicious activity. The framework dictates that only authenticated and authorised users and devices can access applications and data. At the same time, it protects those applications and users from advanced threats on the internet.

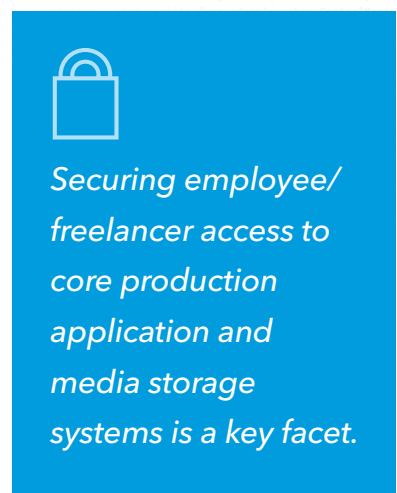
There are several components that companies can use to implement a Zero Trust framework, but securing employee/freelancer access to core production application and media storage systems is a key facet. With such a transitory workforce, media companies face unique challenges in implementing and revoking access to systems, sometimes on a daily basis. With the use of services such as Akamai's Enterprise Application Access, user permissions can be granted easily and quickly to specific applications based on the identity and security context of the user and device, without ever granting users access to the full corporate network.

Another core facet of Zero Trust is implementing systems that proactively identify and block targeted threats such as malware, ransomware, and phishing, which are tools used by pirates in their man-in-the-middle attacks. Akamai's Enterprise Threat Protector, as an example, is a secure web gateway that uses real-time security intelligence to proactively identify and block targeted threats such as malware, ransomware, phishing, and DNS-based data exfiltration.

Protect against geo and IP rights infringements. Another means of acquiring content by pirates is the use of VPN technology to mask their country of origin and IP address. This is typically used following the successful acquisition of a legitimate subscriber's details. Once details have been acquired, pirates then obfuscate their geographical location and IP addresses in order to stream content to multiple locations – a process known as re-streaming. The pervasiveness of VPN services also means that Lazy pirates can easily sign up and access geo-restricted content, e.g., overseas viewers looking to access particular TV episodes. Mechanisms that can be used to protect against this activity include proxy detection technology. Akamai's Enhanced Proxy Detection intelligently blocks requests at the edge associated with anonymous proxy or VPN services.

Protect against playback infringements. This is by far the most popular tactic in the fight against anti-piracy, and can be achieved through a variety of different means, the most prevalent being Digital Rights Management (DRM).

In summary, DRM refers to the tools, standards, and systems used to restrict copyrighted digital materials and prevent unauthorised distribution. It is not a single technology per se. Depending on the criticality of the assets being protected, some distributors are comfortable with simple encryption (i.e., preventing viewers from making copies of videos by writing the content in a code that can only be read by devices or software with the key to unlock the code), as this still requires a “key” to be available providing cursory protection. Keys are typically delivered by HTTP servers, however, and can be copied and shared, so encryption is sometimes not sufficient to protect higher-value content. More advanced DRM technologies handle key communication via a content decryption module using a challenge/response system. These communications are encrypted so the decryption key is never in the open where it can be hacked. Advanced DRM technologies also offer the ability to add business rules that define when and how the keys can be used on different devices such as location, device registration, and time-based rules. As with all technologies, however, there are some challenges when working with DRM technology.



Securing employee/freelancer access to core production application and media storage systems is a key facet.

- a) The first is complexity. Without delving too far into the detail, organisations wanting to implement a comprehensive DRM strategy are required to support multiple technologies, certainly Apple FairPlay, Google Widevine, and Microsoft PlayReady. This is to ensure adequate coverage of the potential browsers, devices, and operating systems available in the market. This introduces cost and complexity into the workflow. Note, via a specification called the Common Media Application Format, the DRM market is moving towards a single set of encrypted files that can support all three technologies, but to date this does not support legacy devices.
- b) The second challenge is the reliance on third-party systems for DRM to operate. If these systems are hacked or DoS'd, then the viewer experience is compromised.
- c) The final area often cited by opponents of DRM is the fallibility of the technology. DRM clearly cannot protect content once it's been decrypted, e.g., screen recording. There have also been instances where specialists have “broken” various DRM technologies to identify flaws. When you are competing against technically proficient, obsessive pirates this should be expected, but should not be a reason to exclude DRM from your strategy.

Many rights owners, certainly those with high-value sports or movies, require distributors to implement some form of DRM protection. The specifications will vary from general guidelines through to exacting requirements. For distributors looking to implement DRM during the packaging process, it's often useful to engage with cloud providers who are able to manage the complexity. Akamai, as an example, has integrated its origin storage for on-demand content with the processing capabilities of several providers, such as Bitmovin and Encoding.com, that are able to implement DRM in near real time. Alternatively, companies are starting to consider the benefits of combining encryption and watermarking as an alternative to DRM. This methodology provides significant benefits with regard to processing costs and viewer experience, but still provides a robust form of playback protection.

Detect

As with any form of theft, protection does not always guarantee success, and as such, detection of infringements are essential. There are several methods of detecting piracy activity in almost real time.

Fingerprinting. Provides the ability to identify video content without modifying the original media. Tools are used to identify, extract, and then represent attributes belonging to a video file, so that any given video can be identified by its unique "fingerprint" – for example, on file-sharing networks. A fingerprint cannot help distinguish between different copies of the same title, i.e., whose copy of a video was leaked in the first instance. As such, the technology is generally used by services such as YouTube's Content ID, to help determine when copyrighted material is uploaded from accounts that do not have the rights to redistribute it. Fingerprinting is also used to help organisations understand the prevalence of piracy of their own content, before a more robust strategy is put in place.

Watermarking. This is now one of the most prevalent forms of piracy detection. While watermarking cannot directly stop piracy, it enables service providers to detect piracy, identify those who engage in it, and do something about it. Essentially, video watermarking consists of adding a pattern of "bits" that are unnoticeable to the human eye and nonremovable, into a video file that you want to authenticate. Linking this data to the identity of the viewer means it is possible to trace a pirate who copies content after it is decrypted and illegally distributes it.

There are three main methods of video watermarking currently in use: bitstream modification, A/B variant, and client-side watermarking.

Bitstream modification involves modifying selected areas of a picture in a way that maintains video quality, but the viewer and session are identifiable. As a methodology, it is robust but requires a significant compute overhead and adds latency into the system, making it unsuitable for live content.

A/B variant watermarking is aimed at the OTT sector. Two identical video streams are created, watermarked, and subsequently interlaced together either client-side or through CDN edge processing, providing a unique identifier. It is a robust, cost-effective method, but as the identifying sequence can be long it is not favored in situations that require quick watermark extraction.

Client-side watermarking is favored for its rapid watermark extraction and ability to deploy across legacy platforms e.g., set-top boxes. A graphical overlay is composited onto the video stream in the client device, which can be made invisible. The watermark is not applied until it reaches the client, and therefore content needs to be safeguarded separately during delivery. Additionally, distributors will need to consider deploying SDKs for OTT devices, which can add operational overhead.

There are numerous forms of watermarking available depending on the use case. A key element to any watermarking strategy, however, is to ensure adequate monitoring is taking place so that adequate enforcement techniques can be applied to pirates. Many anti-piracy technology providers provide managed monitoring services, or advice can be sought from anti-piracy consultancies such as Cartesian, which can assist in developing in-house capabilities.

Akamai works with major watermarking providers to ensure a viable solution can be made available and integrated within an overall video piracy strategy.

Stream log identification. Another form of detection is examining the logs of distribution partners such as CDNs in real time, which can identify piracy activity for livestreams. In this scenario, deep log inspection provides a real-time picture of infringing activity based on authorised and unauthorised IP addresses. The advantage of these solutions, such as Akamai's Stream Protector, is the ability to turn on the capability quickly depending on the situation, and the ability to enforce specific rules. As an example, a broadcaster may have acquired valuable sports rights for a limited period but does not want to invest in watermarking technology. As such, they can use stream log identification to provide a similar level of detection without the upfront workflow or technology costs. The disadvantage of this technology is that it can only be used with one distribution partner, which is a challenge in a multi-CDN environment.

Enforce

When piracy activity has been detected, it's important to then be able to act in an appropriate manner. Depending on your strategy, this can take a number of different directions.

Revoke access. If your video assets are time sensitive, such as sports or other live events, then you will want to revoke access to the originator of the illegal stream immediately or as soon as possible. There are different ways of achieving this. A common methodology is to work with your distribution service provider, exchange relevant details, and stop streaming activity from an offending IP address. If clear operational procedures are in place, this can occur within a reasonable period of time. There are many situations, however, for which time is of the essence – such as high-value sports events, or when the distribution of pirated content can become viral. Akamai provides a service that allows stream revocation in real time and without unnecessary intervention. This has proved particularly effective where piracy monitoring is taking place using either watermarking or stream log identification.



Ensure adequate monitoring is taking place so that adequate enforcement techniques can be applied to pirates.

Stream modification. In less time-sensitive situations, distributors can decide to modify the pirated stream by replacing legitimate streams with alternative content (Big Buck Bunny is popular) or reducing the stream quality. This approach has the benefit of hiding detection from the pirate stream originator and stopping them from jumping to a different stream source.

Real-time messaging. As described in the pirate persona section, Lazy pirates feel safe with the anonymity of the internet. Organisations such as VFT are able to identify viewers of live pirated streams on social media platforms and can message the infringer directly. Using this form of enforcement, distributors are able to modify the enforcement, such as initially offering access to legitimate streams – and if infringement continues, legal notices.

To assist the general education on the topic, there are now increasingly sophisticated real-time message platforms that can target offenders. With the correct anti-piracy services, operators can identify viewers who are watching illegal streams and incentivise them, through soft and hard countermeasures, to switch to legitimate services. Actions can include explaining the impact of their actions, offering commercial incentives to access legitimate streams, or harder countermeasures involving the introduction of law-enforcement authorities. The key here is removing anonymity from the process and actively educating the viewer.

Conclusion

Video piracy over IP is a complex, nuanced subject, but one that has the potential to threaten the long-term viability of the media industry as we know it. There is overwhelming evidence that points towards significant financial damage, but more importantly that piracy has the potential to fundamentally undermine or impact global licensing models.

To date, the response from the industry has been relatively muted, with the burden of fighting pirates fragmented across certain broadcasters, pay TV operators, and industry bodies. As described by one analyst, “We are at the early adopter stage with much work ahead”. An increasing number of distributors have woken up to the threat, and most “tier 1” video producers and operators have now established dedicated teams to better understand piracy, evaluate their own situation, and implement relevant anti-piracy strategies. As described in this document, however, without some form of operational ubiquity and coordination across the industry – coupled with support from governments, regulators, and legislators – this will be a tough fight. Like any battle, one weak link and the effort put in by others is lost.

There are several immediate requirements identified in this paper that are required to help the industry fight the battle. These include consistent piracy data points to help executives and the wider industry understand the threat; continued education of the general public about the wider impact of piracy on jobs, and the threat to national industries; cooperation across anti-piracy vendors and service providers to ensure technical solutions can be integrated efficiently; and, finally, leadership from rights owners across all genres to drive ubiquity across the industry when handling and distributing rights.

The good news is that much of this is starting to mobilise. The EUIPO, as an example, is providing clear data points regarding the extent and impact of piracy across the European Union, using a methodology that could be adopted by other regions. National governments still need to wake up to the problem, but with clearer information on the impact of piracy in place, we can hope to see the implementation of tougher legislation. Vendors are looking at the strengths of combining capabilities. As an example, Akamai – in addition to bringing its cybersecurity expertise to bear – is working with all leading watermarking companies to ensure that once pirates have been detected, their activities can be terminated immediately. Finally, we are seeing signs that rights owners of valuable content are insisting on minimum standards of content protection across the technical workflow. Today these are often isolated instances or “suggestions” (as is the case with the MPAA) – but moving forward, we see these becoming a necessary function of doing business.

With these initiatives in place, we can minimise the issue so that financial losses are reduced, job opportunities are protected, and licensing can continue to thrive in a global marketplace.



Akamai is working with all leading watermarking companies to ensure once pirates have been detected, their activities can be terminated immediately.

REFERENCES

- Asia Video Industry Association. The Asia Video Industry Report. 2019.
- Bevir. Cost of online piracy to hit \$52bn. 2017. Retrieved from <https://www.ibt.org/publish/cost-of-online-piracy-to-hit-52bn/2509.article>
- Blackburn et al. Impacts of Digital Video Piracy on the U.S. Economy. 2019.
- Coberly. Streaming services are 'killing' piracy. Retrieved from <https://www.techspot.com/news/78977-streaming-services-killing-piracy-new-zealand-study-claims.html>
- CustosTech. The Economics of Digital Piracy. 2014.
- Daly. The pirates of the multiplex. Retrieved from <https://www.vanityfair.com/news/2007/03/piratebay200703>
- Decary, Morselli, Langlois. A Study of Social Organisation and Recognition Among Warez Hackers. 2012.
- Digital Citizens Alliance. Fishing in the piracy stream. Retrieved from https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/DCA_Fishing_in_the_Piracy_Stream_v6.pdf
- Enigmmax. Interview with a Warez Scene Releaser. 2007. Retrieved from <https://torrentfreak.com/interview-with-a-warez-scene-releaser/>
- European Commission. Estimating displacement rates of copyrighted content in the EU. May 2015.
- European Union Intellectual Property Office. Trends in Digital Copyright Infringement in the European Union. 2018.
- European Union Intellectual Property Office. Illegal IPTV in the European Union. 2019.
- FACT. Cracking down on digital piracy. 2017.
- Feldman. Article on the use of streaming services. 2017. Retrieved from <https://yougov.co.uk/topics/politics/articles-reports/2017/04/20/almost-five-million-britons-use-illegal-tv-streami>
- FriendsMTS. Comparing subscriber watermarking technologies for premium pay TV content. 2019.
- Frontier Economics. The economic impacts of counterfeiting and piracy. Report prepared for BASCAP and INTA. 2017.
- Granados. Report: Millions Illegally Live-Streamed El Clasico. 2015. Retrieved from <https://www.forbes.com/sites/nelsongranados/2016/12/05/sports-industry-alert-millions-illegally-live-streamed-biggest-spanish-soccer-rivalry/#3544c3f37147>
- Greenburg. Economics of video piracy. 2015. <https://pitjournal.unc.edu/article/economics-video-piracy>

Ibosiola D., Steery B., Garcia-Recureroy A., Stringhiniz G., Uhlgy S., and Tysony G. *Movie Pirates of the Caribbean: Exploring Illegal Streaming Cyberlockers*. 2018.

Intellectual Property Office. *Online Copyright Infringement Tracker*. 2018.

Jarnikov et al. *A Watermarking System for Adaptive Streaming*. 2014.

Jones, Foo. *Analyzing the Modern OTT Piracy Video Ecosystem*. SCTE•ISBE. 2018

Joost Poort et al. *Global Online Piracy Study*, University of Amsterdam Institute for Information Law. July 2018.

Kan. *Pirating 'Game of Thrones'? That file is probably malware*. 2019. Retrieved from <https://mashable.com/article/pirating-game-of-thrones-malware/?europe>

Lee, T. *Texas-size sophistry*. 2006. Retrieved from <http://techliberation.com/2006/10/01/texas-size-sophistry/>

Liebowitz S. "The impact of internet piracy on sales and revenues of copyright owners", an abridged version of "Internet piracy: the estimated impact on sales" in *Handbook on the Digital Creative Economy* Edited by Ruth Towse and Christian Handke, Edward Elgar. 2013.

Mick, J. *Nearly half of Americans pirate casually, but pirates purchase more legal content*. January 21, 2013. Retrieved from <http://www.dailytech.com/Nearly+Half+of+Americans+Pirate+Casually+But+Pirates+Purchase+More+Legal+Content/article29702.htm>

Motion Picture Association of America. *The Economic Contribution of the Motion Picture & Television Industry to the United States*. November 2018.

MPA Content Security Program. *Content Security Best Practices Common Guidelines*. Motion Picture Association. 2019.

MUSO. *Measuring ROI in content protection*. 2020.

Nordic Content Protection Group. *Annual Report, 2020*.

Parks Associates. *Video Piracy: Ecosystem, Risks, and Impact*. 2019.

Tassi, P. April 15, 2014. "Game of Thrones" sets piracy world record, but does HBO care? Retrieved from <http://www.forbes.com/sites/insertcoin/2014/04/15/game-of-thrones-sets-piracy-world-record-but-does-hbo-care>

Sanchez, J. January 3, 2012. *How copyright industries con congress*. Retrieved from <http://www.cato.org/blog/how-copyright-industries-con-congress>

Sandvine. *Video and Television Piracy*. 2019.

Schonfeld. *Pirate Bay makes \$4m a year*. 2008. Retrieved from <https://techcrunch.com/2008/01/31/the-pirate-bay-makes-4-million-a-year-on-illegal-p2p-file-sharing-says-prosecutor/>

Sulleyman. *Pirate Treasure: How Criminals Make Millions From Illegal Streaming*. 2017. Retrieved from <https://www.independent.co.uk/life-style/gadgets-and-tech/news/piracy-streaming-illegal-feeds-how-criminals-make-money-a7954026.html>

Techspot. *Streaming services are killing piracy*. Review of Vocus group research. 2019. Retrieved from <https://www.techspot.com/news/78977-streaming-services-killing-piracy-new-zealand-study-claims.html>

Torrentfreak. *Making Money from Movie Streaming Sites, an Insiders Story*. 2013. Retrieved from <https://torrentfreak.com/making-money-from-movie-streaming-sites-an-insiders-story-131019/>

VFT. *Pirate Persona Whitepaper*. 2014.

Walters, B. *Interview with Helen Mirren*. Time Out London. Retrieved from <http://www.timeout.com/london/film/interview-with-helen-mirren>



Akamai secures and delivers digital experiences for the world's largest companies. Akamai's intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps, and experiences closer to users than anyone – and attacks and threats far away. Akamai's portfolio of edge security, web and mobile performance, enterprise access, and video delivery solutions is supported by unmatched customer service, analytics, and 24/7/365 monitoring. To learn why the world's top brands trust Akamai, visit akamai.com, blogs.akamai.com, or [@Akamai](https://twitter.com/Akamai) on Twitter. You can find our global contact information at akamai.com/locations. Published 07/20.