

Taking the Offensive Against Video Piracy

Piracy Models, Anti-Piracy Technologies and Best Practices Continue to Evolve as Awareness Increases

A Technical Paper prepared for SCTE•ISBE by

Steven Hawley
Founder and Managing Director
Piracy Monitor
Advanced Media Strategies LLC
Bonney Lake, WA 98391
steven.hawley@piracymonitor.org
+1 (360) 897 6677

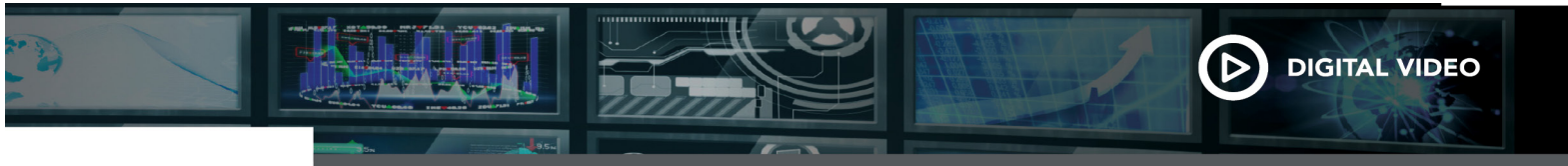
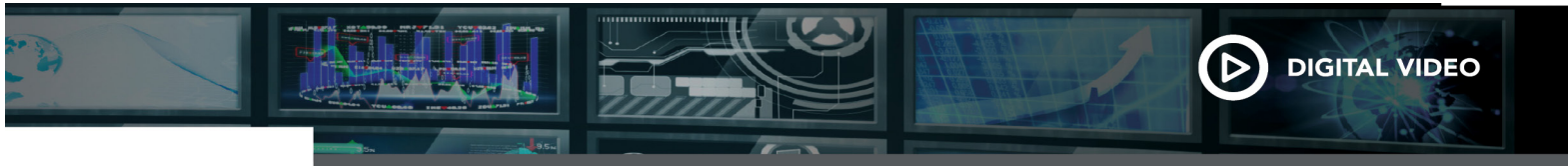


Table of Contents

Title	Page Number
Table of Contents	21
1. Introduction	22
2. What is Video Piracy and How Big is the Problem?	22
3. What is Being Pirated and How?	23
4. Vectors for Piracy	23
5. Piracy Use-cases: How Pirates Reach Consumers	24
5.1. Device environments	24
5.2. Pirate Business Models	25
5.3. Deepfakes, an Emerging Piracy Use-case	26
6. Anti-piracy as a Technical Process	27
6.1. Detection and Analysis: The Evolution of Analytics	27
6.2. A Piracy Decision Loop	28
6.2.1. Credential Monitoring and Analytics	29
6.2.2. Forensic Watermarking and Monitoring	30
6.2.3. Automated content recognition	30
6.2.4. Additional Monitoring Techniques	31
7. Anti-piracy: The Long Game	31
7.1. Elements of an Anti-Piracy Program	31
7.2. Technical Guidelines	32
8. Conclusions	32
9. Bibliography and References	34

List of Figures

Title	Page Number
Figure 1: Pirate Video Service with a Tiered Subscription Model (Source: IPTV Nitro)	26
Figure 2: Analytics for video quality, advertising and rights infringement (Source: Piracy Monitor)	28
Figure 3: Monitoring to detect out-of-profile service usage (Source: Piracy Monitor)	29
Figure 4: Piracy monitoring, detection, decision and action (Source: Piracy Monitor)	30



1. Introduction

Over the past several years, online video piracy has rightfully attained a higher profile in the consciousness of the video industry. The evolution of video analytics platforms used by operators and video providers has been a reflection of this awareness. Pay TV service providers have focused their concerns on reducing the unlicensed use of legitimate services within their service reach, while content providers going direct-to-consumer (OTT) or reaching consumers via online aggregators have focused more on identifying content that is found outside of its legitimate channels of distribution on the Internet.

There also is a growing awareness that the technologies used to identify infringing use, the application of anti-piracy countermeasures, and the decision process that triggers anti-piracy responses must be complemented by well-informed business rules and business policies that guide the selection and use of anti-piracy technology. A complete anti-piracy program also consists of executive level commitment, operational practices and organizational resources that are dedicated to anti-piracy, as well as a network of collaborators in the Internet community and in law enforcement.

Piracy falls into three categories: the theft of content, the theft of services, and theft of advertising. Rather than providing a deeply technical discussion of any particular aspect of video piracy, this article takes three steps back to look at the bigger picture.

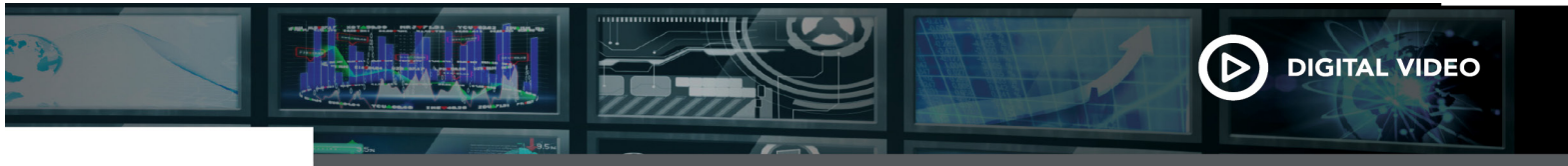
2. What is Video Piracy and How Big is the Problem?

Video piracy is the distribution of stolen video content or the redistribution of stolen services, without the rights to do so. Theft can occur as a result of breaches to data centers, video processing and storage, the process of delivery, by breaching the user authentication process, or through capture at the time of playback.

According to a report published by Parks Associates in January 2020, the value of pirate video services accessed by pay TV and non-pay TV consumers may exceed \$67 Billion worldwide in 2023.¹ If just 10 percent of pay TV subscribers discontinued pay TV services in favor of video delivered by pirates, the 2023 loss to operators could approach \$6 Billion. This is in addition to services revenue lost by pay TV operators due to password sharing. The broader impact of global piracy in the US was estimated to be more than 29 Billion in 2018 alone, by the US Chamber of Commerce.²

Even individual piracy cases are quite valuable. For example, in 2019, a piracy operation called Omniverse One World Television,³ which offered video via a Web portal, through resellers, and via a custom-built illicit streaming device - and even sold advertising - was shut down. In October 2019, Omniverse agreed to pay a \$50 Million settlement. In October 2018, SetTV paid damages of more than \$90 Million to US satellite TV provider DISH Network and NagraStar, as the penalty for distributing programming stolen from DISH to more than 180,000 users. SetTV was shut down.¹

Password (credential) sharing has been seen by the industry as something of a gray area. Some will say that the sharing of credentials outside of the scope of granted *usage* permissions is piracy, even if access is not shared further. Others contend that password sharing isn't piracy unless it is done with the intent to *redistribute* content without the rights to do so. It is not the purpose of this article to settle this question with a legal opinion. In isolated instances, some will even allow infringement as an intentional marketing tactic to boost viewership.



In any case, credential sharing results in significant lost revenue to pay TV operators. A survey of US consumers conducted by Parks Associates earlier in 2019⁴ determined that 5% and 6% of those surveyed used someone else's credentials to access pay TV and online video services, respectively. Other estimates are higher.

3. What is Being Pirated and How?

Today, any type of content that can be turned into digital bits is subject to online piracy. Measured in terms of links that are propagated by pirates, more than half of pirated content is television programming, followed by movies (about a fifth of all content), software (about a tenth), games (about a tenth), and published content such as e-books (most of the remainder), according to private research by Piracy Monitor.

If we look at TV programming alone, sports makes up about three quarters of the content delivered via streams that are propagated by pirates. Within the sports genre, football (soccer) is unsurprisingly the most pirated, followed by general sports programming (networks that carry multiple sports), followed by basketball and motorsports. Beyond the sports genre, the most stolen content is TV series and movie programming.

Advertising is also subject to fraudulent use by video pirates, in two ways. The greater threat to advertisers comes from the theft of legitimate advertising by pirates. A CNBC report about a pirate video service called TeaTV⁵ described how the service tricked automated advertising services into serving legitimate ads to it programmatically. In such situations, not only is the pirate taking payments under fraudulent pretenses, but also, the fact that the advertiser becomes associated with the pirate may do damage to the advertiser's brand and reputation.

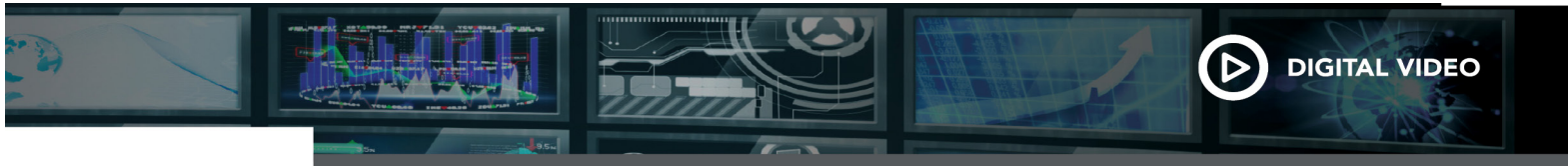
The other form of advertising fraud is by fraudulent video providers, to gain prominent placement within search engine results. Try an online search for "IPTV" and you will see.

4. Vectors for Piracy

The avenue to piracy that has captured the most attention by pay TV operators has been the fraudulent use of end-user credentials, which is essentially a theft of *service*, and not directly the theft of content. To be clear, the act of consumers sharing passwords - or using passwords shared to them by others - is not where most of the credentials used for industrial-scale piracy originate.

The more widespread form of piracy results from the theft of *content*. A variety of methods are available to pirates to capture content, ranging from old-fashioned video camcording in movie theatres and HD television sets, to theft of digital production copies and DVD ripping. Another way is to overcome traditional pay TV conditional access safeguards. A pirate can steal programming at the point of reception by using decoders and stolen keys to decrypt incoming satellite signals.

To identify TV channels with a high likelihood of being stolen, such as a premium pay-per-view event, the video provider can embed invisible forensic watermarks into the video computationally. If the content has been watermarked, pirates can use a process called "collusion" to average a set of multiple instances of the same channel to defeat the watermark before re-encoding it into streaming formats for redistribution.



Large-scale content theft results from the theft of aggregated service credentials. Pirates use consumer databases that were stolen through accidental breaches or the intentional penetration of enterprise data centers and made available for purchase on the Dark Web. These databases may have been stolen from pay TV providers, retailers, financial services institutions, or from other consumer-facing enterprises. Another method is to leverage social media APIs to expose consumer data.

In turn, this consumer data can be used as the basis for phishing attacks upon consumers, in which a pirate masquerading as a legitimate video provider sends a message asking the consumer (for example) to log in and re-set their password. This conveys actual account access to the pirate, which, in turn, opens the potential to steal directly from the video provider's library.

Another way to access video libraries using consumer credentials is to use brute force. Because many consumers use the same user-IDs and passwords for all of their online accounts, credentials from non-media account sources can bear fruit, so pirates will use automation to keep trying account credentials until they find ones that work.

5. Piracy Use-cases: How Pirates Reach Consumers

Once the pirate has acquired the content, video pirates leverage several physical delivery methods:

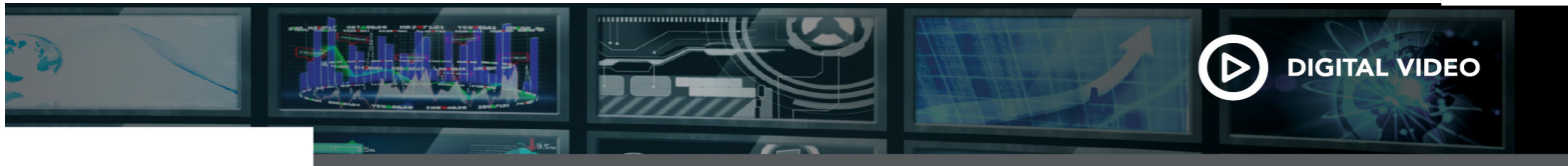
- “IPTV” streaming¹ which, in terms of the proportion of overall pirate distribution, has increased steadily in recent years. Streaming is more prevalent in North America and Europe
- Direct file download, which is prevalent in Asia, Latin America and Africa and has decreased in recent years
- Peer-to-Peer (torrent) distribution, which is more prevalent in South Asia and Oceania and has also decreased
- Digital lockers, which are file storage services that can host files for download, FTP transfer or torrenting

5.1. Device environments

Consumer environments targeted by pirates include:

- Pay TV set-top boxes where programming is intercepted at output
- Retail streaming devices (such as Roku, Fire TV, et al.), PCs, game consoles, mobile smartphones and tablets, and smart TVs.
- Browsers that reside in PCs and game consoles, accessing pirate streaming Web sites
- Apps that run in legitimate media center environments such as Kodi, which consist of pirated online video and multichannel TV programming. Kodi is available for PCs, game consoles, mobile devices and Raspberry Pi.
- Apps developed by pirates that run in Android and iOS consumer devices, to present pre-linked stolen programming to smartphone and tablet users.

¹ “IPTV” – Traditionally, the term Internet Protocol Television and its acronym IPTV have been used to reference pay TV services delivered through IP multicast over operator-managed networks; originally by the Telcos. It is a supreme irony that this term has been pirated by the pirates, and has become the generally recognized term for pirate video streaming.



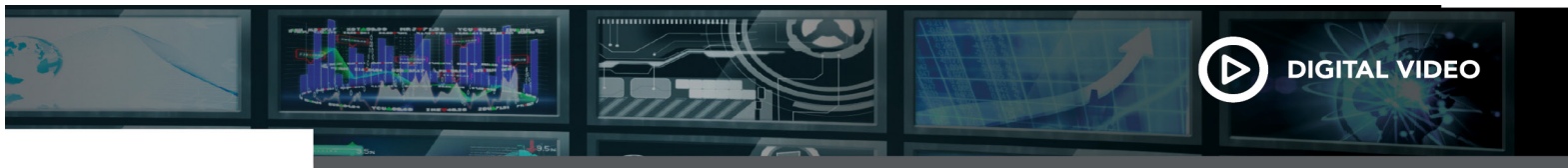
- Illicit streaming devices (ISDs) which are custom-designed, produced in quantity, and sold at retail or online. They are preconfigured with an embedded Web browser that is pre-programmed to access pirate video streams. Often, these devices also offer private app stores that allow users to download jailbroken or illicit versions of apps that redistribute legitimate services. Content may be free or at additional cost

Another form of video acquisition by pirates is the capture satellite programming at a receiver, to convert into streams for redistribution.

5.2. Pirate Business Models

Pirates make money by leveraging one or more business models, which include:

- Free-to-consumer model: Some pirates establish Web sites to aggregate pre-programmed links to streaming servers that are hosted by others, into a single user experience that can be accessed from any browser. These sites are often free to the consumer, and funded by fraudulent use of programmatic advertising. Alternatively, they may be funded by revenue shared by providers of ransomware that is surreptitiously distributed via the streaming portal and installed on the consumer's device.
- "Pay TV" subscription model: Some pirates create streaming services with tiered bundles that resemble a pay TV service. Often, these will have "good," "better," and "best" ranges of programming, and will charge a different amount for each programming tier. Revenue comes from monthly payment. The consumer may pay for access using an online payment account or cryptocurrency
- Business-to-Business model: Some pirates assemble turnkey services that are not intended for direct-to-consumer streaming, but rather, host and present stolen content for streaming, direct file download, or P2P (torrent) distribution by resellers. This approach has appeal because multiple resellers amplify the pirate's market presence. The appeal to the reseller is that the reseller does not host any content directly, but rather, acts as a linking site.
- Combination model: Some pirates will do a combination of some or all of the above. One example is Ominverse One World Television, which offered an Android-based ISD with an embedded appstore directly to consumers. It also offered its delivery infrastructure and content to multiple resellers, many of which believed Omniverse to be legitimate. Its programming was a combination of pay TV and online video programming and sold ad insertion space to legitimate multichannel TV advertisers.



Pirates have become increasingly sophisticated and attract consumers with low prices and high production values. One example is in Figure 1 below. In most regions of the world, consumer awareness has been such that most consumers can't discriminate between legitimate and pirate services.

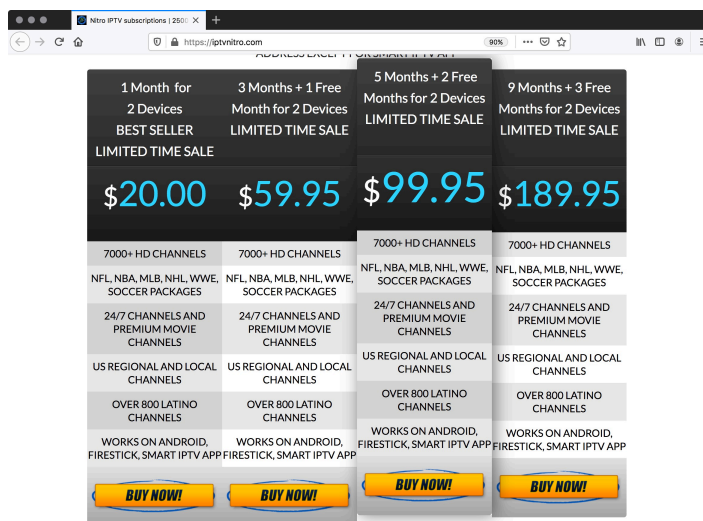


Figure 1: Pirate Video Service with a Tiered Subscription Model (Source: IPTV Nitro)

A comprehensive reference paper about illicit streaming devices, satellite signal re-encoding and other methods used by pirates to steal and deliver video to consumers can be found in the 2018 SCTE-ISBE paper *Analyzing the Modern OTT Piracy Ecosystem*.⁶

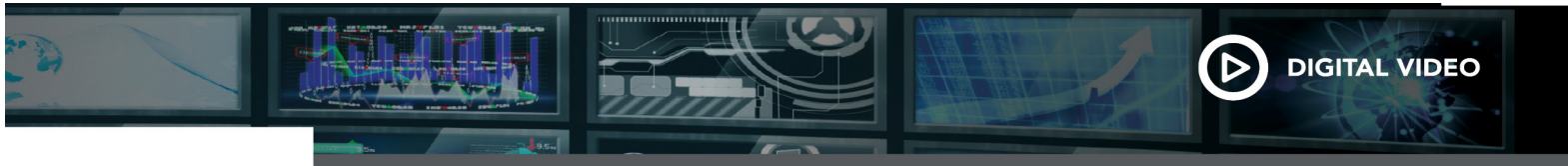
5.3. Deepfakes, an Emerging Piracy Use-case

An additional emerging threat is that of deepfakes, which are video clips or programs that are designed to deceive the viewer. Deepfakes can be used to spread disinformation about a given topic or brand by making changes that are relatively easy to make, given today's content production tools.

Stolen content can be embedded within a deepfake video during production. Techniques have also been developed by smartphone providers to create full videos from single still image frames (selfies, for example). The audio track of a video or still image using a trusted spokesperson can be edited or replaced, and the spokesperson's facial expressions can be revised. The fraudulent result may be so good as to be indistinguishable from fact by humans.

Deepfakes can also be produced to attack independent content creators, where images or video content developed by the independent creator can be modified, using an attacker's audio content, for example. The attacker can then approach the independent creator, charge them with theft of its audio track, and extort a ransom for "copyright."

If the source content has been watermarked prior to release, it can be detected if it is used within a deepfake, so the deepfake can be taken out of circulation or its producer prosecuted.



6. Anti-piracy as a Technical Process

Anti-piracy is a combination of detection and action. The process of detecting suspected instances of piracy and then confirming (or dismissing) them as infringing use is automated through the use of monitoring and analytics. Once detected and confirmed, the instance is presented for decision and action.

6.1. Detection and Analysis: The Evolution of Analytics

Video providers have long endeavored to provide high quality service. The pursuit of video quality has changed over time, but the goal has always been in service of the video provider's overall value propositions to consumers. In other words, to make the video experience look and work better.

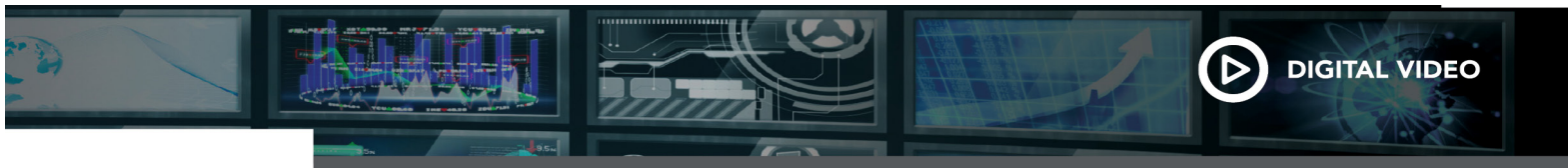
Video analytics began with the test and monitoring of quality of service (QoS), which is mainly about minimizing delivery errors. This provided a foundation to improve quality of experience (QoE), by measuring the integrity of the content, including video clarity, adherence to color gamut parameters, audio/video sync, captioning, and metadata, and the overall presentation of the experience. Good QoE is dependent upon good QoS.

As video services migrated to Internet Protocol access, it became possible to use the technologies of online ad insertion, ad measurement and streaming quality analytics to better ensure continuity of experience and to measure its effectiveness: advertising analytics.

To detect and address piracy, analytics has taken another step. Video providers can establish usage parameters, watch for usage that falls outside of those parameters, and monitor for content originating from sources that are suspected of piracy to see where that content came from (e.g. was it stolen from your service? From which device and which end user account?). This can be referred to as infringement analytics.

To stay abreast of the constant barrage of monitoring data, automation is necessary to determine whether or not to raise a red flag. Evaluation parameters are typically established by the content rights-holder or content owner. Examples include:

- Number of devices: Allowing account holders to use a defined number of simultaneously active devices. Detecting sudden changes in the range or number of devices associated with an account.
- Allowed devices: to permit delivery to specific types of devices (e.g. HD STBs and streaming devices, but not smartphones).
- Location of use; for example, in-home use only or attempts to access services from unrecognized locations.
- Registered devices: to detect when someone whose device is not registered in a subscriber's household attempts to watch a program – with or without access credentials.
- Anomalous service usage: for example spikes in service access or license requests in a short period of time
- Anomalous content attempts: for example, to make requests through broken or nonexistent links (the equivalent of a Web '404'). Or requests to unrecognized IP address ranges, VPN links, or unrecognized NAT-ted addresses
- ...and others



Infringement analytics platforms are also equipped not only to evaluate watermarks, but also to evaluate fingerprints (automated content recognition, video metadata, operator and content provider logo images, and monitor known infringing sites on an ongoing basis.

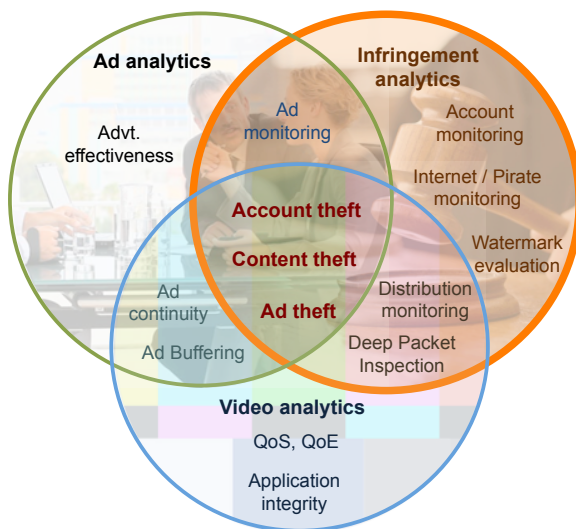
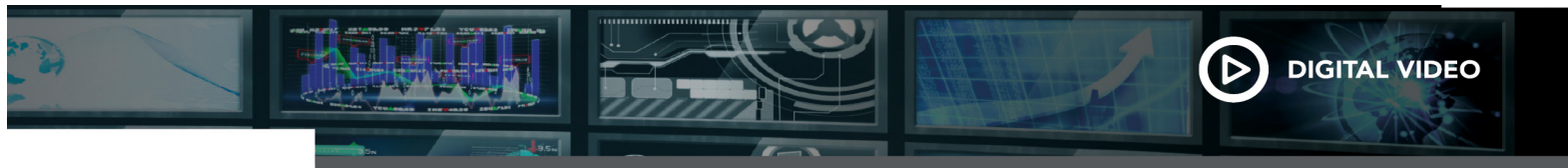


Figure 2: Analytics for video quality, advertising and rights infringement (Source: Piracy Monitor)

Together, these three approaches - video analytics, advertising analytics and infringement analytics - combine to ensure an overall high-quality experience that conforms to rights parameters.

6.2. A Piracy Decision Loop

Once in place, the technical side of anti-piracy is a process of monitoring, detection, alerting, and then, to apply a desired outcome. There are several methods for doing this.



6.2.1. Credential Monitoring and Analytics

One method is in Figure 3 below, in which an analytics platform is in place to detect the distribution and use of a video service or stream. The platform can detect the user's location, device profile, and other identifying information, to detect infringing use.

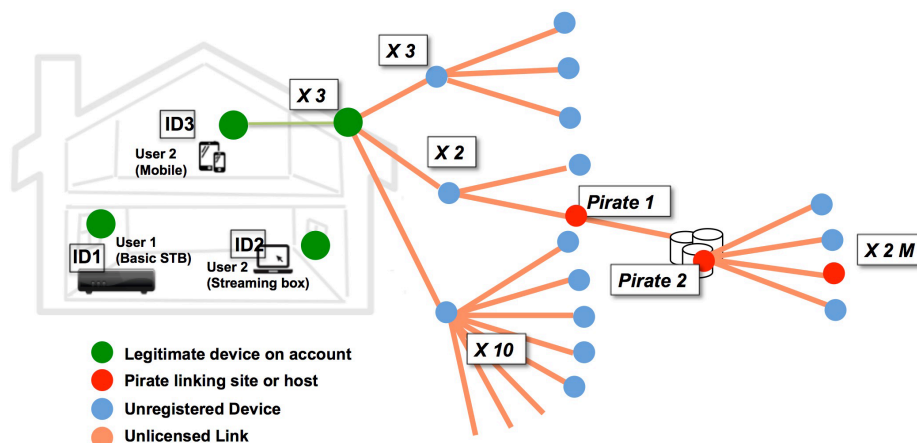
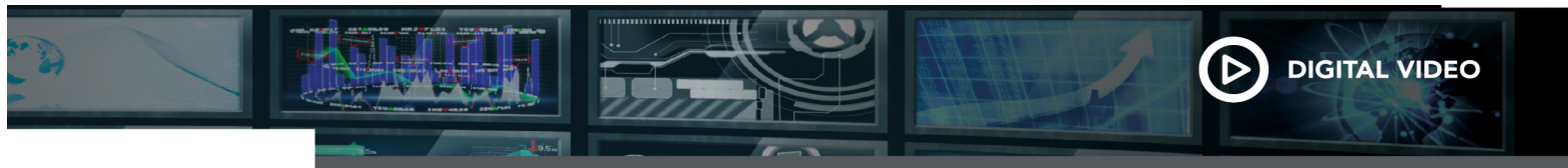


Figure 3: Monitoring to detect out-of-profile service usage (Source: Piracy Monitor)

Users #1 and #2 within the household pictured at left are all legitimate registered users and all of the devices are registered with the service. User #2 is sharing to another receiving device or user within the household. Monitoring and analytics show that this recipient was in turn sharing the service with three other devices or users. One of them, in turn, shared to 3 others. Another shared to 10 others. And while the third user shared to just two others, one of them was a pirate that used that shared access to steal content that was, in turn distributed to a hosting pirate site that served 2 million end users.

Video providers can build 'typical' user profiles for a streaming video account, which then provides a reference point used to detect out-of-profile account usage.



6.2.2. Forensic Watermarking and Monitoring

Rather than monitoring for service abuse, Figure 4 below shows the process of monitoring for stolen content. To begin, the content is prepared for distribution by embedding a forensic watermark. If a video asset is suspected of distribution by a pirate, the video can be evaluated individually for the presence of that particular watermark.

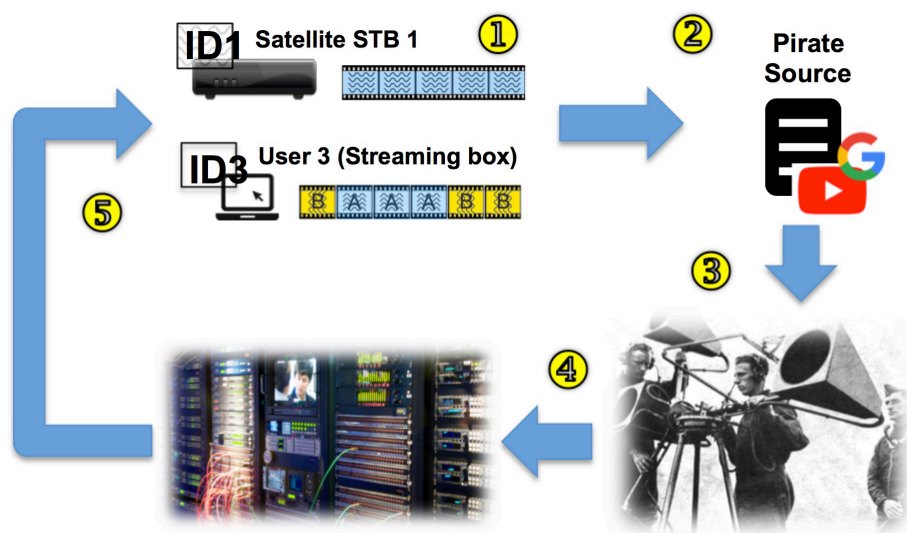


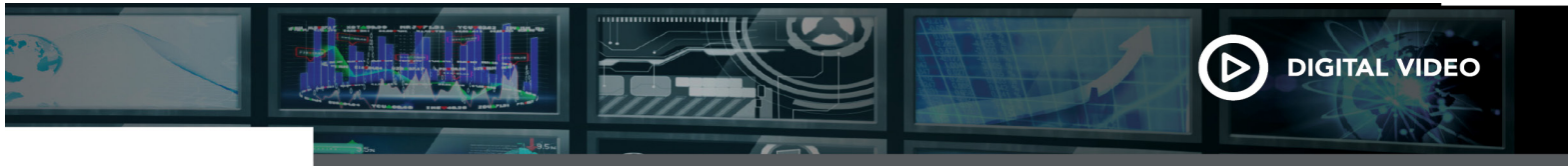
Figure 4: Piracy monitoring, detection, decision and action (Source: Piracy Monitor)

In Step 1 of Figure 4, content is watermarked. This watermark may be embedded at the point of encoding to identify a program that is distributed via broadcast or multicast, as with the video being played by the satellite set-top box. Alternatively, the watermark may be embedded when a streaming session is established, at the service provider's headend or in the CDN. In this example, watermarking is a two step process that first creates duplicate streams with given different watermarks and then segmented. Each streaming session assembles the video segments in a sequence that is unique to that session. Alternatively, watermarks can be applied by a software process running within the streaming client device (not pictured), which eliminates the need for duplicate streams; in turn, reducing the need for storage and processing resources.

In Step 2, a pirate has intercepted the video and is distributing it over the Internet. Step 3 shows the originating video provider monitoring suspected pirate sources for instances of its video content. The monitoring platform has been programmed to alert the video provider (Step 4) that a video is suspected of having been stolen. Upon confirmation, through an automated or a human decision making process, the keys to the device are revoked or the stream is shut down (Step 5).

6.2.3. Automated content recognition

Also known as fingerprinting, automated content recognition (ACR) is in some ways the “inverse” of watermarking: a process used to extract tiny fragments from a video asset without changing the source content itself, and then store these fragments in a database that associates it with an owner or authorized distributor.



Through automation, the video content found on the Internet is compared against the fragments in the database. If it identifies sources that were not licensed to distribute the content, the system signals the legitimate owner or distributor.

6.2.4. Additional Monitoring Techniques

Other anti-piracy approaches include deep packet inspection and evaluation of network flow data. By looking at the request and handshaking process within a video request, a monitoring platform can detect out of range IP addresses, unauthorized virtual addressing, the use of VPNs or proxies, or packet characteristics that may indicate infringement.

Additional reference material is available in past papers published by SCTE-ISBE, including:

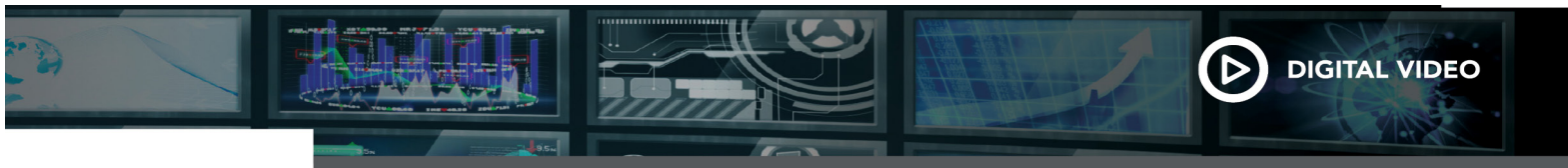
- Detecting Video Piracy with Machine Learning (2019)⁷
- Automated Detection for Theft of OTT Services and Content (2017)⁸
- Service Theft in DOCSIS Networks (2019)⁹

7. Anti-piracy: The Long Game

As noted earlier, a complete anti-piracy initiative complements detection and analytics technologies with policies, practices and organizational development. Content protection and anti-piracy technical guidelines are available from multiple sources.

7.1. Elements of an Anti-Piracy Program

Task Force	Establish a dedicated Anti-piracy Team consisting of executive management, with designated technical, financial, marketing and legal experts who are tasked with overseeing, approving and enacting the anti-piracy initiative
Strategy and Goals	Produce an anti-piracy strategy and a set of anti-piracy goals. Develop policies designed to accomplish those goals
Solutions Owner	Empower a program manager to work cross-functionally within the company, to define an anti-piracy initiative and to shepherd it through conceptualization, requirements-development, vendor selection, implementation, operationalization and ongoing improvement.
Risk Assessment	Commission an end-to-end security audit and systems analysis to investigate and confirm the nature and scope of vulnerabilities to piracy. Assess traditional pay TV security and digital rights management as well as IT infrastructure. Consider outside resources with anti-piracy expertise.
Architecture	Establish a reference anti-piracy framework based on risks, goals and policies, informed by the risk assessment, and by technical and financial feasibility analysis. Recommend a first choice and a fallback approach from among multiple possible solutions.
Resources	Determine the program elements, resources and enabling technologies that best fulfill goals and policies.



Operations	Develop a dedicated operations resource responsible for piracy, with a reporting process, a severity-ranking system, and escalation and resolution procedures. Consider building a simulation environment to replicate attacks and to evaluate alternative solutions.
Cybersecurity	Because many piracy risks exist outside of video processing and delivery, identify points in data centers and in the cloud where content, personally identifiable information and internal resources could be exposed to exploitation or compromise
Intelligence	Evaluate emerging piracy, anti-piracy and cybersecurity use-cases on an ongoing basis, to continually improve those practices. Stay abreast of regulation that may affect you.
Community	Join organizations from the media, entertainment and technology industries that focus on piracy in your region. Sign up for their infringement and piracy alerts. Establish relationships with search engines and other online providers that may have contact with your content or services.
Law Enforcement	Gain an understanding of the governmental and regulatory agencies with jurisdiction in your own territory, as well as for those in regional and global markets (such as the European Union); and for international law enforcement agencies such as Interpol. Identify your local liaison officers.

It is also important to recognize that the piracy problem is not static. Pirates and hackers are very creative and live in a culture where smart people challenge other smart people to create more effective traps. Some of them are individuals that operate in the dark, while others are nation-state actors. Some of them eventually decide that their energies are better used to join the fight against piracy.

7.2. Technical Guidelines

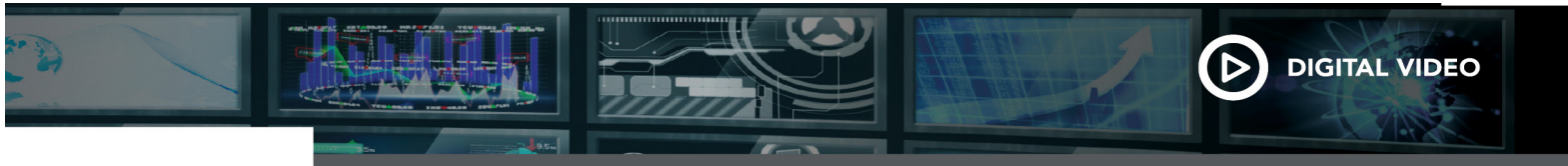
In addition to the MovieLabs recommendations noted earlier, several other media industry organizations publish guidelines for content protection and antipiracy. They include:

- *The Enhanced Content Protection Specification*, from MovieLabs ¹⁰
- *Content Protection Best Practices*, from the Motion Picture Association (MPA/MPAA) ¹¹
- *The Ultra HD Forum Guidelines*, ¹² from the Ultra HD Forum
- *Forensic Watermarking Implementation Considerations for Streaming Media*, from the Streaming Video Alliance ¹³

8. Conclusions

In today's streaming video world, piracy is a fact of life. The US Chamber of Commerce estimated the impact of global online piracy to the US economy in 2018 to be more than \$29 Billion in lost revenue. According to a 2019 study released by Deloitte, ¹⁴ 2018 marked the first year that streaming video captured more consumers than traditional TV.

While credential theft and account abuse have been the focus of pay TV operators and online content aggregators, content owners and producers have been more concerned with theft of the content itself, no



matter whether it is the result of theft of OTT services or of a breach to delivery infrastructure or consumer devices.

High-value content is more likely to be stolen, where value is measured by exclusivity, choice, immediacy, age and quality.

Exclusivity: Programming that is exclusive to a single programmer is more likely to be stolen. Consider *The Mandalorian*, the *Star Wars* series that was introduced with the launch of Disney+ by The Walt Disney Company in the US, Canada and the Netherlands in November 2019. Streams were detected by Google Trends in many other countries almost immediately after Disney+ went live.

Choice: With the emergence of so many SVOD streaming services, consumers have to choose. It is becoming more and more likely that any given consumer will want *something* that is not available via the services that they subscribe to, so the consumer might attempt to access it from a pirate source rather than pay for yet another SVOD service.

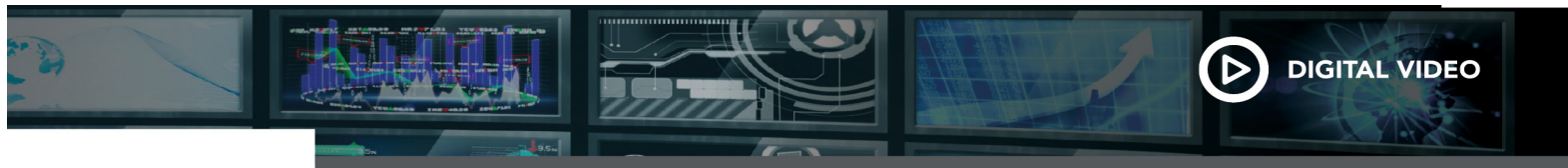
Immediacy: Pay-per-view live sports programming is most valuable when a match or a game is in its early stages. This makes it incumbent on sports programmers and video providers that carry that programming to be in a position to detect illegal streams, isolate their sources, and take action in minutes.

Age: The age of the content is critically important. Just as media companies stage the distribution of their content in different release windows for different distribution channels, with the most valuable windows coming first; new releases are more likely to be pirated

Quality: Because ultra high-definition programming has become more mainstream, UHD resolution has become less of a differentiator and therefore is less likely to justify a higher fee just because it is UHD. However, UHD quality also enables a pirate to generate high quality streams that nullifies any differentiation based on quality by legitimate online video providers. This is why Movielabs, MPAA and others have issued formal guidelines for forensic watermarking, to be able to detect stolen UHD content and make it easier to take it out of circulation.

Digital piracy as we know it today arguably had its origins nearly 20 years ago with the emergence of music hosting sites like Napster and KaZaA, which hosted stolen audio content for download using peer-to-peer protocols. In retrospect, Apple's iTunes service was probably the legitimate alternative that had the most impact in reducing music piracy while enabling content owners and rights-holders recapture some of the revenue that had been lost to pirates.

For video, a similarly disruptive 'silver bullet' solution has yet to emerge.



9. Bibliography and References

¹ Hawley, Riney, Kent. *Video Piracy: Ecosystem, Risks and Impact*. Research report. Parks Associates. January 2020. See: <https://www.parksassociates.com>

² Blackburn, Eisenach, Harrison. *Impacts of Digital Video Piracy on the US Economy*. Research report. NERA Economic Consulting and the US Chamber of Commerce Global Innovation Policy Center. June 2019. See: <https://www.theglobalipcenter.com/wp-content/uploads/2019/06/Digital-Video-Piracy.pdf>

³ *Complaint for Copyright Infringement. Demand for Jury Trial*. Legal complaint against Omniverse One World Television, a pirate operation. United States District Court. Central District of California. Western Division. February 14, 2019. See: <https://www.documentcloud.org/documents/5740024-Omniverse.html>

⁴ Naden, Jiang, Kamble. *360 Deep Dive: Account Sharing and Digital Piracy*. Research report. Parks Associates. July 2019. See: <https://www.parksassociates.com/blog/article/pr-07162019>

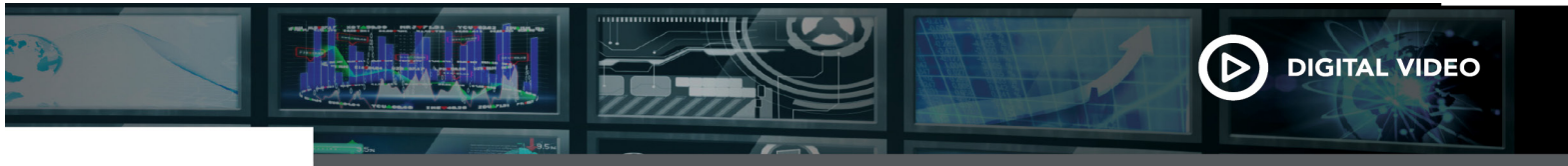
⁵ Megan Graham. *Netflix and HBO shows are getting pirated on this app that's been bankrolled by advertisers such as Pandora, BET+ and TikTok*. Article. CNBC. October 20, 2019. See: <https://www.cnbc.com/2019/10/20/netflix-and-hbo-shows-are-getting-pirated-on-teatv-and-other-sites.html>

⁶ Jones (Comcast), Foo (Charter). *Analyzing the Modern OTT Piracy Ecosystem (2018)*. White Paper. SCTE-ISBE. September 2018. See: <https://www.nctatechnicalpapers.com/Paper/2018/2018-analyzing-the-modern-ott-piracy-video-ecosystem>

⁷ Tooley, Belford. *Detecting Video Piracy With Machine Learning (2019)*. White Paper. NCTA. September 2019. See: <https://www.nctatechnicalpapers.com/Paper/2019/2019-detecting-video-piracy-with-machine-learning>

⁸ Catranis, Yuan, Belt (Irdeto). *Automated Detection for Theft of OTT Services and Content (2017)*. White Paper. NCTA. 2017. See: <https://www.nctatechnicalpapers.com/Paper/2017/2017-automated-detection-for-theft-of-ott-services-and-content>

⁹ Westervelt, Florendo, Belt (Irdeto). *Service Theft in DOCSIS Networks (2017)*. White Paper. NCTA. 2017. See: <https://www.nctatechnicalpapers.com/Paper/2017/2017-service-theft-in-docsis-networks>



¹⁰ *Movielabs Specification for Enhanced Content Protection*. Technical Guidelines. Movielabs. Revised 2018. See: <https://movielabs.com/solutions-specifications/enhanced-content-protection-ecp/>

¹¹ *Content Protection Best Practices*. Technical guidelines document. Motion Picture Association. October 2019. See: <https://www.motionpictures.org/what-we-do/advancing-creativity/additional-resources/#content-protection-best-practices>

¹² *Ultra HD Forum Guidelines*. Technical guidelines document. Ultra HD Forum. September 2019. See: <https://ultrahdforum.org/guidelines/>

¹³ Stevenson (Ericsson), Wilkenson (Comcast). *Forensic Watermarking Implementation Considerations for Streaming Media*. Technical guidelines document. Streaming Video Alliance. July 2018. See: <https://www.streamingvideoalliance.org/books/forensic-watermarking-implementation-considerations-for-streaming-media/>

¹⁴ *Digital Media Trends Survey, 13th Edition*. Report. Deloitte. March 2019. See: <https://www2.deloitte.com/us/en/insights/industry/technology/digital-media-trends-consumption-habits-survey/summary.html>