It's Showtime!

Innovation explodes across every workflow as technology emerges from the pandemic.

Where are you in this accelerated evolution?

DIVERSITY & INCLUSION
In the office, behind the camera, and on the screen, diversity is crucial

SECURITY
Remote productions create new security concerns, with assets under siege

SMART CONTENT
Artificial intelligence and machine learning are being applied in new, exciting ways

NEW WORKFLOWS
The cloud is delivering on its promise, powering the future of productions

21.01

NEXT GENERATION CONTENT PROTECTION: MOVING BEYOND IP FOR LOCATION VERIFICATION

Geolocation verification methods can save content owners billions

ABSTRACT: Faced with ever-evolving techniques to spoof an IP address, moving beyond IP for viewer location verification is becoming increasingly important for protecting geographically restricted content, especially when it comes to high-value content. Location signals from Wi-Fi, GPS, and HTML5 can now be used to stop geo-piracy and geolocation fraud.

By James Clark, Director, Global Sales, GeoGuard

Let's face it: there's never been a better time to be a streaming video service provider.

Content consumption via streaming services is at an all-time high, and there's no sign of it slowing down. A recent report by Juniper Research predicts that by 2025, there will be close to 2 billion OTT TV and video subscribers worldwide. That's a 65 percent increase from 2020. By those estimates, there's no denying we are definitely entering the golden age of streaming.

Unfortunately, legitimate consumers aren't the only ones with an insatiable appetite for binge-worthy TV and high-stakes live sporting events. Digital pirates can't seem to get enough either, and by all accounts, they're salivating at the thought of even more content to pilfer.

Parks Associates is forecasting that in 2024, pirates will siphon off a staggering $12.5 billion in revenue from OTT and pay TV companies. That's a growth rate of 38 percent from the estimated $9.1 billion lost in 2019.

Clearly, piracy cannot be dismissed as the cost of doing business. There's just too much at stake, especially for premium content producers. So, as we look to the future, what can studios, sports leagues, content creators and premium OTTs do to mitigate these losses, as well as maintaining their content's value while upholding their contractual obligations?

According to a recent report published by the Streaming Video Association (SVA), forward-thinking OTTs should consider implementing a robust and layered security framework that includes tighter geographical barriers: "Poorly implemented restrictions allow consumers to access content outside the permitted territories for free and/or at a reduced price than the licensed distributor price (e.g., a boxing match in Ireland costs $25 vs. $80 for the same match in the U.S.)."

HOW PIRATES BOLDLY BYPASS TERRITORIAL RESTRICTIONS

When it comes to tightening up security around territorially restricted content, the SVA is careful to point out that "addresses cannot" be solely relied upon to make decisions as IP databases are often inaccurate and IP addresses can be masked with virtual private networks (VPNs)."

Approximately, three in 10 internet users use a VPN service, and more than 50 percent of those VPN users admit that their primary goal is to spoof their location in order to access territorially restricted content. Traffic to VPNs (one solution provider claims to have over 140 million customers), is driven by OTT video content popularity.

To stop this kind of piracy (aka geo-piracy), you need to implement proven tools like GeoGuard's Database

> *BLOCKING ARMCHAIR PIRATES from accessing your content illegally is one thing. What about the more pervasive, tech-savvy cyber-criminals who have an array of anonymizing tools at their disposal?*

solution. This Hollywood studio-approved VPN and DNS proxy detection solution has been third-party tested and found to be 99.6 percent effective against the industry's most popular VPNs. Plus, it's already used by broadcasters and premier OTT providers globally and integrated with world-leading CDNs including Akamai and Amazon AWS. It's quickly become the recommended solution of many studios, sports leagues, broadcasters and rightsholders.

Protecting content from geo-fraud is an area Akamai explores further in its recent white paper, "Inside the World of Video Pirates — How Do We Stop Them?" In the white paper, Akamai notes: "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."

GEO-FENCING IN THE NEW PIRACY UNIVERSE

Blocking armchair pirates from accessing your content illegally is one thing. What about the more pervasive tech-savvy, cyber-criminals who have an array of anonymizing tools at their disposal? In the same way that VPNs can spoof a user's location via an IP address, there's a growing number of fake location apps and spoofing techniques designed to circumvent more advanced location validation methods, including:

■ **Disabling Wi-Fi and installing SIM cards from permitted territories**

James Clark leads sales for GeoGuard's geolocation and geo-circumvention detection solutions. He is responsible for identifying opportunities with customers, establishing strategic partnerships, and communicating GeoGuard's products and services to the market. solutions@geoguard.com @geoguard_

■ **Downloading fake location apps or HTML5 browser add-ons to falsify coordinates**
■ **Streaming from a smartphone, where the IP shows up as the location where the phone was registered — not where the device actually is**

Faced with these ever-evolving techniques to spoof location, moving beyond IP for viewer location verification is becoming increasingly important for protecting geographically restricted content — especially when it comes to higher-value content such as pay-per-view live sports or online movie premiers.

In order to outsmart these new spoofing techniques, OTTs will need to utilize advanced geolocation solutions that can verify the true location of a viewer via multiple data sources including Wi-Fi, GPS, GSM and HTML5, along with real-time and historic risk analysis.

Granted, this approach may seem a little heavy-handed for low-value content. But, as the SVA points out, when it comes to big-ticket sporting events and highly anticipated movie releases, not adopting stronger geolocation verification methods could cost studios, sports leagues, rightsholders and premium OTTs billions in lost revenue.

GeoGuard's core geolocation and fraud detection technology was originally developed for the highly regulated and exacting U.S. online gaming market, where ensuring the true location of a player is critical to complying with state and federal laws. However, this technology is highly adaptable and configurable in order to meet the specific needs of the streaming video industry to combat the ongoing and evolving geo-piracy threat.

Long story short, if we want the entire streaming ecosystem to live long and prosper, we need to consider geo-blocking an essential part of our security and anti-piracy strategies. ⊞

Geolocation Fraud and Geo-Piracy from VPNs and DNS Proxies is hurting the entire streaming ecosystem.

But you can STOP IT!

▶ **Trusted by** industry leaders in the OTT and broadcasting industries

BBC iPlayer · prime video · The CW · PCCW® · Roku

▶ Seamless integration with multiple CDNs, including **Akamai** and **AWS CloudFront**

Akamai · amazon cloudfront

▶ Detect and block **VPN/DNS Proxies** from accessing geographically restricted content

▶ Protect the **territorial exclusivity licensing** you rely on for revenue

▶ Tested and rated as **99.6% effective** by Kingsmead Security

▶ VPN/Proxy database updated **multiple times per day**

GEOGUARD
Fraud Has No Place To Hide

VPN · 3RD PARTY TESTED · STUDIO APPROVED

GeoGuard.com | solutions@GeoGuard.com