PART THREE
NEXGUARD IS TOOL OF CHOICE
IN ALL WATERMARKING SCENARIOS

Rights Holders Gain Speed & Reliability in Fighting Content Theft Worldwide

WHITE PAPER - DECEMBER 2017
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>03</td>
<td>INTRODUCTION</td>
</tr>
<tr>
<td>04</td>
<td>TRENDS BEHIND A GROWING NEED FOR EFFECTIVE USE OF WATERMARKING</td>
</tr>
<tr>
<td>04</td>
<td>The Impact of Connected TVs on the Pirated Video Viewing Experience</td>
</tr>
<tr>
<td>05</td>
<td>Bandwidth Trends Supporting OTT Streaming of 4K UHD Content</td>
</tr>
<tr>
<td>06</td>
<td>THE ESSENTIAL ROLE OF WATERMARKING ENABLED BY NEXGUARD</td>
</tr>
<tr>
<td>06</td>
<td>Solutions Tailored for all Distribution Scenarios</td>
</tr>
<tr>
<td>07</td>
<td>The Vital Starting Point</td>
</tr>
<tr>
<td>09</td>
<td>Enabling Rapid Identification of Pirates</td>
</tr>
<tr>
<td>09</td>
<td>The NexGuard Pay-TV Solution for STBs</td>
</tr>
<tr>
<td>10</td>
<td>Ensuring Pirate Identification on all Unmanaged Devices</td>
</tr>
<tr>
<td>11</td>
<td>Fully Automated and Blind Detection</td>
</tr>
<tr>
<td>12</td>
<td>CONCLUSION</td>
</tr>
</tbody>
</table>
The urgency behind the premium video industry’s need for a forensic watermarking solution that encompasses every usage scenario in the multiscreen marketplace is no longer in dispute.

The role NAGRA’s NexGuard watermarking platform and forensic services play in battling illicit streaming of online sports and other linear programming as described in Part Two of this series dovetails with growing recognition that content owners are making watermarking technology a basic requirement in the licensing of premium video content across all outlets. This marks a significant change in the industry’s perspective on watermarking from where it stood just a short time ago.

Scenarios tied to distribution of motion pictures in 4K UHD over legacy pay TV outlets that motivated the issuance of Enhanced Content Protection (ECP) specifications by the Hollywood studios’ MovieLabs in 2013 have been materializing gradually. As 4K UHD enhanced by high dynamic range (HDR) technology delivers a significantly superior viewing experience that is sure to supplant HD over time, the industry’s commitment to thwarting piracy will drive ever greater reliance on watermarking as an essential deterrent against the extension of this viewing experience to users of purloined content.

Where movies are concerned, the situation is about to change dramatically by the end of 2017 with the introduction of early release windows for VOD. The studios are ready to make movies available electronically much earlier via premium VOD services. However, to protect downstream revenues, they strictly mandate the use of watermarking.

Beyond such developments, as rights holders place ever greater reliance on the revenue-generating potential of live sports and other content streamed in HD, which we documented in Part One, the scale of online piracy has created an even more immediate need for an effective watermarking solution. The real-time nature of live sports calls for a level of automation and speed in responsiveness never envisioned with the use of watermarking in scenarios involving non-live content.

As these concerns shape licensing requirements for delivering premium video across all outlets, it’s essential that distributors of every stripe undertake the due diligence, testing and other measures essential to making the right watermarking technology choices. As shall be seen in the discussion that follows, NexGuard used in conjunction with the NAGRA anti-piracy and legal services described in Part Two satisfies every requirement for the use of watermarking at all points of vulnerability in the distribution chain.
THE IMPACT OF CONNECTED TVs ON THE PIRATED VIDEO VIEWING EXPERIENCE

One of the most serious areas of concern when it comes to dealing with illegal sports streaming centers is the fact that pirates are able to achieve quality levels suited to viewing the content on big TV displays. Consumers at home strongly prefer to watch movies and sports on such screens rather than PCs or mobile devices.

With the high penetration of broadband and legal OTT services in developed countries, consumers have gotten used to viewing this content on TVs either through streaming devices or direct connections built into the sets. In the U.S., as of the start of 2016, 45% of U.S. broadband households owned at least one smart (connected) TV, up from 34% a year earlier, and 36% owned at least one streaming media player compared to 27% a year earlier, according to Parks Associates.¹

The same trends are in play elsewhere. By 2019, smart TV penetration in many countries besides the U.S. will be above the 50% mark, including Japan at 63%, Germany and the U.K. at 53% and France at 50%, according to projections from U.K. researcher IHS.²

In other words, pirated content is now available for high-quality viewing as part of OTT consumption on big-screen displays throughout much of the world.

The appeal of using connected TVs to view online video is heightened by the fact that virtually all sets on sale in retail stores with 40” or larger screens support 3840 x 2160-pixel 4K resolution. According to researcher Strategy Analytics, global penetration of 4K TV sets will be close to 50% by the end of 2020.³ HD content received by these sets is automatically enhanced by various techniques to achieve quality that comes close to matching content produced in 4K.

Pirates are avidly exploiting these trends. Whereas they used to focus streaming primarily on PCs and mobile devices, now they are targeting TVs as well by adopting the same consumer streaming technology used by Roku, Apple TV and other TV streaming devices. They rely on open source software like Kodi to make it easy and cheap for consumers to see illegally streamed content on their big screens.

Pirates can be expected to ride the next wave of video quality enhancements now getting underway with the emergence of HDR (high dynamic range). HDR-enabled 4K UHD displays, now widely available on multiple models from leading manufacturers, deliver a dramatic improvement in the viewing experience in conjunction with HDR-capable content.

Figure 2: Consumers at home strongly prefer to watch movies and sports on TV screens rather than PCs or mobile devices

Figure 3: Sports broadcasters are moving rapidly to embrace the technology now that there’s a growing market base of HDR TV owners
The availability of HDR-infused 4K UHD content so far has been limited to online offerings, primarily with original content from Netflix and Amazon. But producers, including sports broadcasters, are moving rapidly to embrace the technology now that there’s a growing market base of HDR TV owners. Critically, the emergence of HDR has led to a growing consensus within the TV industry that there’s an ROI upside to offering 4K UHD services.

A recent global survey conducted by SNL Kagan found that 64% of MVPDs and 73% of content producers among the nearly 500 respondents believe consumers will be willing to pay 10% to 30% more on their subscriptions for access to 4K UHD content. Ninety-six percent of those respondents said they believe 4K UHD TV services will be widely adopted by 2020.

**BANDWIDTH TRENDS SUPPORTING OTT STREAMING OF 4K UHD CONTENT**

Paralleling these changes in TV technology and content is the expansion of broadband access rates to levels that are sufficient to support mass market reach for OTT content delivered in the new formats. The amount of bandwidth required to deliver 4K UHD with use of a next-generation compression such as MPEG’s HEVC (High Efficiency Video Coding) varies from about 18 Mbps, the bitrate Netflix has set for streaming its HDR-enhanced 4K content, to 25 Mbps for live sports streams, as evidenced with the launch of sports streaming services by BT and Sky in Europe.

At the current rate of broadband bandwidth expansion throughout much of the world it appears likely that a vast share of users will be able to access live streamed 4K UHD sports content as it becomes more widely available. According to CDN operator Akamai, 12% of all requests for Web content from users served by Akamai’s global CDN infrastructure were fulfilled at connection speeds of 25 Mbps or higher in the first quarter of 2017, representing a 16% increase from the previous year.

A quarter of all connections worldwide are already operating at 15 Mbps with proportions much higher in many countries. These include the U.S., where 42% of sessions recorded by Akamai operated at 15 Mbps or above, and ten other countries, led by South Korea at 64%, where the percentage operating at 15 Mbps or better reached or topped 44%.

High throughput on the return paths of broadband fixed and mobile networks also will provide pirates, including casual users, more bandwidth to upload the stolen content from ever more points of capture. With billions of smartphones, tablets and laptops equipped with high-resolution cameras and the ability to transmit at speeds exceeding 100 Mbps, pirates will have all the bandwidth they need to maximize the quality of content restreamed from these devices.
For reasons spelled out in Part One and Two of this series, the use of forensic watermarking to identify the source of a leak has already become an essential component in the anti-piracy toolkit. Amid gathering momentum behind the emergence of 4K UHD formatted content in legacy and online domains, it’s clear that the supplanting of HD by the next generation of TV display technology will soon add even greater urgency both to licensors’ demands and to licensees’ needs for support from forensic watermarking capabilities. These are available through NexGuard and the previously described forensic and legal services that NAGRA can uniquely provide at global scale to address all live sports and TV programming usage scenarios that are vulnerable to in-the-clear capture and restreaming by professional and amateur pirates.

**SOLUTIONS TAILORED FOR ALL DISTRIBUTION SCENARIOS**

Ideally, to maximize the benefits of the technology, producers and distributors will want to make use of watermarking at all stages in the distribution chain to identify the source of a leak wherever it occurs, whether it happens in post-production, at the point of broadcast playout, at distributor facilities or at end-user locations. NexGuard solutions have been tailored to meet the specific requirements of each scenario, with options including File Delivery for file distribution watermarking, Network ID for live broadcast distribution path watermarking, NexGuard PayTV for set-top-box client-side watermarking and NexGuard Streaming for OTT watermarking.

In all instances, the speed at which NAGRA’s forensic teams can utilize the NexGuard watermark to identify sources of piracy is an advantage customers can’t obtain elsewhere by virtue of the tie-in between NAGRA’s proprietary fingerprinting service and NexGuard.

As discussed in Part Two, NAGRA uses forensic fingerprinting technology to enable immediate identification of any content offered by a customer that appears on a pirate service. This makes it possible for the anti-piracy service to bypass the time-consuming search for metadata that otherwise would have to be used to confirm that the purloined content violates rights held by the customer rather than another entity.

---

**Figure 4:** Producers and distributors will want to make use of watermarking at all stages in the distribution chain to identify the source of a leak.
The combined use of fingerprinting and watermarking also helps to eliminate errors that typically occur through reliance on metadata retrieval to verify identity of the rights holder. This is one reason NAGRA is able to achieve the avoidance of false positives in the forensics process, which, as mentioned in Part Two, equates to less than a billion-to-one chance of error in identifying sources of illicit activity.

Whatever type of NexGuard solution is deployed, the platform’s digital coding processes produce watermarks that have been shown under rigorous lab and field testing worldwide to be impervious to removal or detection by third parties, even in the high-resolution and dynamic range environment associated with 4K UHD content. These tests have also demonstrated the fact that NexGuard watermarks remain detectable to authorized forensics experts through severe degradations of the content, beyond the point that it has any commercial value.

The imperceptibility of the NexGuard watermark has also been validated by major movie studios, content owners and pay-TV operators.

These validations have been performed by staff members at these entities who are designated as “golden eyes” by virtue of their perceptual acuity to verify content quality in postproduction.

THE VITAL STARTING POINT

NexGuard solutions can be implemented by any given provider and its affiliates step by step starting with watermarking by the content owner at the point of origin and followed by individual distributors using NexGuard to uniquely associate content with specific end users, or the different layers can be implemented all at once. Either way the watermarks implemented at these different staging can be layered on top of each other without compromising the ability to read them individually.

Even without use of watermarking to associate content with specific end users, it’s important to recognize there are major benefits to be realized with use of the NexGuard Network ID solution farther back in the distribution chain. This is the ideal starting point for broadcasters and other content originators in a climate where infringement on providers’ rights can come from any corner of the globe.

The ability to identify geographical areas of origination goes a long way toward helping NAGRA’s forensics experts find the perpetrators. By spotting a watermark embedded into a broadcaster’s contribution feed that can be traced through the delivery chain to the point of local MVPD or over-the-air distribution, the NAGRA teams can narrow and greatly accelerate the search for the illicit source using the other forensic methods described in Part Two.
NexGuard’s Network ID solution makes this possible through a high-level, light approach that maximizes effective tracking across multiple layers in the distribution system. Content owners can identify licensees, typically premium channel outlets, where attacks against the content have occurred, and the content owners or their licensees can identify any points of attack occurring at cable, satellite, broadcast station, OTT or other outlets in the licensee’s distribution chain.

The detection capabilities extend worldwide to provide content owners the ability to identify any local outlet in the distribution workflow where theft has occurred.

In all cases, the extremely high-quality forensic watermark supplied through Network ID is immediately identifiable by NAGRA’s forensics teams as a mark specifically associated with the broadcast-to-affiliate tier of distribution.

Figure 6: NexGuard Network ID one-to-one distribution model and Network ID one-to-many distribution model
ENABLING RAPID IDENTIFICATION OF PIRATES

At the end-user level, the NexGuard PayTV and NexGuard Streaming solutions cover all the bases essential to identifying specific perpetrators wherever they operate. Here it’s important to note that when it comes to MVPDs’ application of watermarking at the per-session level in today’s multiscreen pay-TV services, operators’ activation of these capabilities will likely depend on confirmation that they will be required to do so under licensing requirements imposed by their programming affiliates. Consequently, for best results, content providers who plan to introduce such requirements should let their MVPD partners know their intentions as far in advance as possible to ensure timely implementation of the watermarking infrastructure.

In some instances, the programmer, i.e., the premium channel owner, also operates one or more of its own distribution outlets. NAGRA, in providing its solutions to such entities, has found that by implementing watermarking with their own distribution outlets they create pressure on other distributors to meet the watermarking requirement, since not to do so would be to cede the audience for that channel to the outlets that are using the technology.

The NexGuard PayTV Solution for STBs

In the case of the initiation of theft on legacy broadcast or OTT multicast channels delivered through STBs, it’s necessary to be able to insert watermarks through mechanisms activated at the STB level. Effective implementation requires use of a watermarking integration that is as close to ubiquitously available as possible, even in MVPD environments where multiple STB brands and models might be in use.

There are two approaches to activating NexGuard PayTV, depending on whether or not NexGuard has been embedded in the STB system-on-a-chip (SoC).
Owing to NexGuard’s longstanding position as the leading provider of forensic watermarking for the pay-TV industry, manufacturers of STB SoCs across the globe, including virtually all suppliers of SoCs for 4K STBs, have incorporated support for NexGuard PayTV watermarking in products now running OEM STBs in tens of millions of households. NexGuard PayTV was designed to support implementation in accord with each SoC maker’s specifications, enabling activation with simple download of a trusted application. As a result, MVPDs and virtual MVPDs can be sure they’ll be able to meet licensors’ requirements for watermarking 4K content with use of NexGuard PayTV no matter which OEMs they rely on for their 4K STBs.

In instances where STBs are not running on SoCs embedded with NexGuard, the technology can be integrated into the STB software stack via standard procedures that are used to download software upgrades to deployed STBs. It’s also important to note that, with the ease of use with embedded SoCs or via software upgrades to STBs, NexGuard PayTV offers providers of unicast OTT content the option of relying on STB-based watermarking as an alternative to server-side watermarking with NexGuard Streaming.

**Ensuring Pirate Identification on all Unmanaged Devices**

NexGuard Streaming provides the support for server-side insertion of watermarks on a per-session basis, ensuring that providers will be able to identify sources of piracy no matter what type of Internet-connected device is used to capture and transmit the stolen content. NexGuard Streaming works across all major streaming modes and DRMs and can be scaled to apply watermarking to any number of content streams, depending on the provider’s needs.

In addition, NexGuard Streaming is fully compatible with CDN (content distribution network) technology with the capability to run on CDN appliances or...
externally to them. The per-session watermarking process is added as a step to the manifest file generation workflow, ensuring that the placement is consistent with how ABR [adaptive bitrate] streams are fragmented.

**Fully Automated and Blind Detection**

The cloud-based highly scalable NexGuard Live Detection service works in tandem with session-based tracking as well as with Network ID to enable identification of live re-streaming of protected sports content within minutes after the stream launches. The service, which is available to Web monitoring service providers or to premium sports channel operators employing in-house monitoring, is operated by NexGuard leveraging the Amazon Web Services cloud.

NexGuard’s Live Detection service does not rely on traditional “non-blind” approaches to watermark detection, which require comparison of the watermarked video with original non-watermarked source material and related metadata in order to extract the marks. Instead, the service employs a “blind” approach that extracts the marks directly from the video without reference to source material, thereby enabling quick action against pirated live content. As a result, the service is able to look for a watermark payload in a constant stream of video and return the unique identifier for the source of the pirate stream within minutes.

This opens two avenues providers can pursue to terminate user access to illegally streamed content. If, through watermarking, a subscriber to the original content provider is discovered to be re-streaming the content illegally, the provider can stop the activity by simply switching off the subscriber. Alternatively, through NAGRA’s affiliation with CDN operators and ISPs worldwide, notifications resulting from identifying illegally sourced streams can be used to generate immediate blockage of the flows on those facilities.
CONCLUSION

As documented in Part Two of this series, all the capabilities embodied in the NexGuard platform are leveraged by NAGRA’s forensics and legal teams to provide rights holders an unprecedented level of effectiveness in the fight against piracy wherever it occurs throughout the world.

The combined force of NexGuard and other technical innovations in the hands of experts who are able to work with CDN operators, ISPs and local authorities to speed action against illegal transmission of sports and other content enables customers to maximize prospects for success with whatever courses they decide to take, including court action. And when there’s a need to engage the courts, they can tap legal support from NAGRA that applies understanding of local laws, procedures and precedents born of long experience battling piracy on every continent.

Today the comprehensive forensic watermarking solutions provided by NexGuard are becoming essential weapons in the anti-piracy arsenal. But in short order, content owners of live sports and premium VOD movies will mandate these capabilities for the licensing of high-value video content for distribution through pay-TV, over-the-air and OTT outlets as 4K UHD takes hold as the successor to HD.

Seen in this light, the course for distributors of every description is clear. By putting NexGuard to use sooner than later, they will accelerate their ability to deny pirates the opportunity to stream live sports and other stolen content to users. In doing so, distributors will be able to avoid challenges to their ability to deliver the highest value content as new licensing requirements emerge.

---

I: Yahoo Finance, Parks Associates: Adoption of Internet-Connected Entertainment Devices, September 2016
III: Strategy Analytics, Ultra High Definition TV Displays: Global Market Forecast, March 2015
V: FlatpanelsHD, Netflix Is Now Streaming in HDR, April 2016
VII: Akamai, State of the Internet Report, May 2017