WHITE PAPER

Stopping Geolocation Fraud and Content Leakage via VPNs and DNS Proxies

Best practices and methodologies for OTTs and rightsholders to stop piracy and maintain content value

GEOGUARD

Fraud Has No Place To Hide

Content

This white paper highlights and recommends methodologies and best practices that both OTT broadcasters and rightsholders can implement to stop piracy, protect the value of their digital content and ensure contract compliance.

The white paper is structured into three main sections which can also serve as the basis for specific recommendations for rightsholders to implement in their organization.

Executive Summary

With premium video streaming services growing rapidly in popularity, it's more important than ever to ensure your content is protected from geo-piracy and geolocation fraud initiated from users spoofing their true location via VPNs, DNS proxies and other location spoofing techniques.

For OTT broadcasters, content leakage and geo-piracy via VPNs and DNS Proxies puts them at potential breach of their territorially based content distribution contracts with rightsholders and undermines pricing strategies.

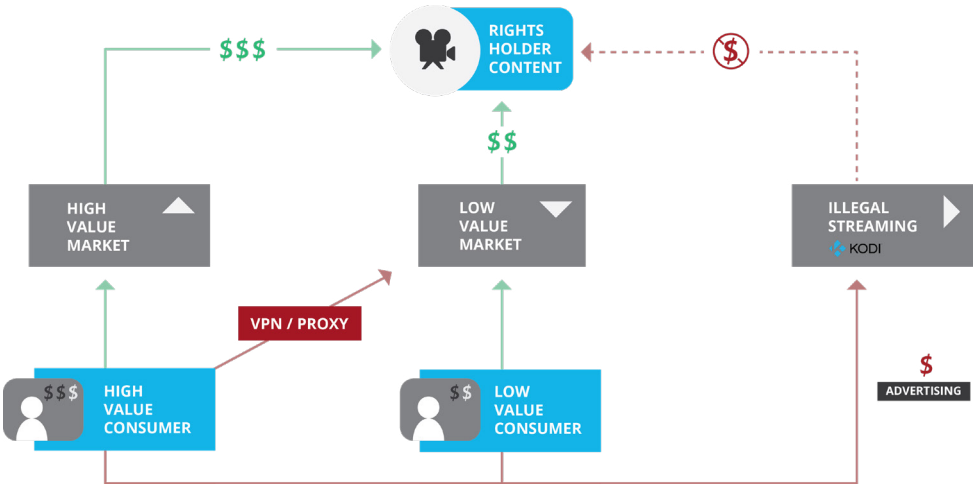
For rightsholders, geo-piracy erodes the value of their content, putting production budgets at risk as well as the ongoing economic viability of their operations.

OTT broadcasters have to contend with a digital grey market of cross-border viewers.

OTT access is multiplatform; consumers typically login via a web browser, iOS device, Android device, Smart TV or streaming device. This makes consistent, cross-platform location detection challenging for OTT broadcasters since consumers have at their disposal a wide range of cheap (or free), easy-to-use, solutions to spoof their location online. As a result, protection needs to be applied evenly across all the popular digital touchpoints – target one method and consumers will simply switch to the next weak link in the chain.

This wide spread use of location spoofing undermines the industry's business model, whereby premium OTT and traditional Pay-TV broadcasters' customers are switching to better value foreign broadcasters who offer the same or better content at cheaper prices or earlier release schedules. Left unchecked, this results in less competition for future broadcast rights and ultimately, lower revenues for future content creation.

Price Arbitrage Risk



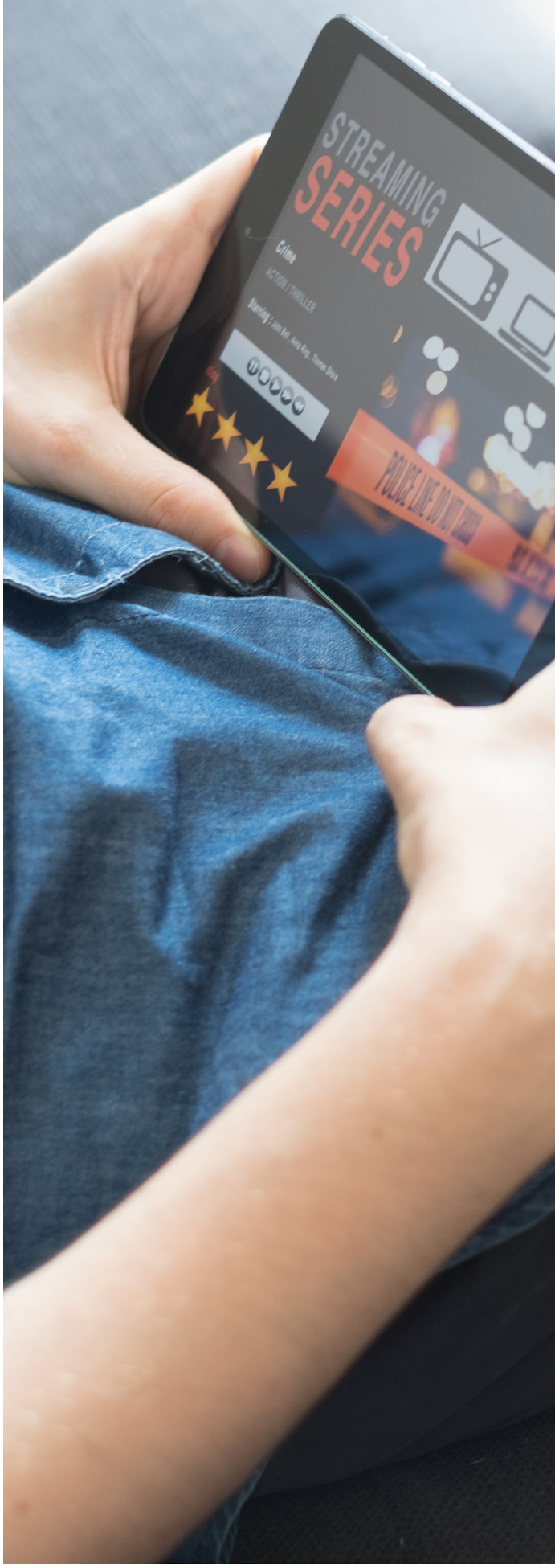
This problem is similar to the grey market which developed during the satellite broadcast era. To take the Canadian and US markets as an example, until 2002, Canadian consumers were legally allowed to receive US Dish Network and DirecTV signals since hacking set-top box decryption cards was a legal grey area. A thriving market sold the relevant hardware to Canadian and US consumers alike - at the expense of broadcasters. In the end, following litigation by Bell Express Vu – a Canadian satellite Pay-TV broadcaster, the Canadian Supreme Court ruled it was illegal to access such services. In this modern-day equivalent (compared to getting a satellite dish set up and buying a pirated access card), just switching on a VPN with a credit card in order to shop around for content cross-border, makes this grey market business a significantly greater risk than it was in the satellite era. Hence, we see hundreds of millions of online users opting to watch cross-border content via a VPN*.

Understand the Scale and Scope of Geo-Piracy Across Digital Touch-Points

Don't OTT broadcasters already check end-user location?

Geolocation checking based on a users' IP addresses is currently the most popular method among OTT broadcasters. However, due to a lack of commonly agreed/applied standards, often the geo-fencing techniques applied is undermined by:

- Use of a cheap/free/poor supplier of geo-IP data
- Use of no/poor VPN detection
- Use of no/poor DNS Proxy detection
- Failure to differentiate between cellular and landline Internet connections. Cellular connections only resolve the IP geo-check to the location of the carrier's base station, not to the user's actual location. This allows roaming customers to appear to be in their home location regardless of their actual location.



- Failure on the part of the OTT broadcaster to integrate properly with their geo-fencing vendors (and sometimes, not at all). This includes inadequate refresh rate of the VPN/Proxy database (once a day, for example, is not enough) and/or not checking at the content delivery network (CDN) layer.
- Failure on the part of the OTT broadcaster to share traffic data/collaborate with the VPN/Proxy detection vendor in such a way as needed to close down the most popular/agile of the VPNs and Proxies. This does not require much effort on the part of the OTT broadcaster but is certainly necessary to assist the vendor in ensuring they are able to quickly respond to new threats.
- Failure on the part of the OTT broadcaster to collect network status on the Smart TV app they are using and thus the inability to see DNS Proxies set at the device/router level.

Did You Know?

GeoGuard is Integrated with Industry Leading CDNs

GeoGuard's advanced VPN and DNS Proxy detection is now integrated directly with some of the world's largest CDN providers, including Akamai and AWS CloudFront. These integrations make it even easier for you to implement an effective solution to combat geolocation fraud and content piracy via VPNs. If you're utilizing Akamai, AWS CloudFront or any other CDN, please contact us at solutions@geoguard.com for more information.

Akamai

Contact

amazon cloudfront

Buy Now

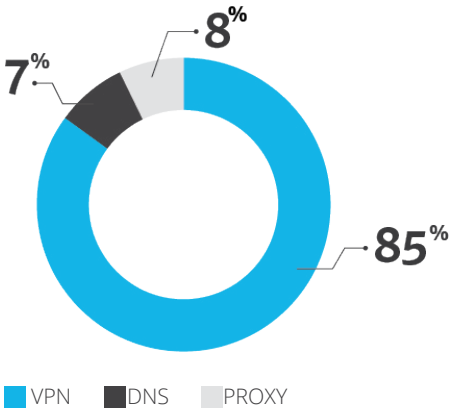
Consumers have several options at their disposal to access content outside of their home territory:

Location Method & Spoofing Method	Description
IP Geolocation - Virtual Private Networks (VPNs)	A VPN is a common tool used to add security and privacy to private and public networks in order to mask the user's IP address. Thousands of sites offer easy to use, one time setup VPN services that will allow the user to hide their location. VPNs are increasingly popular and due to VPN blocking attempts, now even offer residential IP addresses.
IP Geolocation - DNS Proxies	A DNS proxy server enables a client, such as a computer or mobile device, to access region-restricted or blocked content from anywhere in the world. A connection between the client and the site serving restricted content is established through a proxy server located within the approved areas for accessing the content (via streaming, download, etc.).
IP Geolocation - False results due to Mobile Connections	IP addresses collected over a mobile network connection (e.g. 3G, 4G, LTE, 5G etc) are assigned randomly by the mobile ISP and bear no association with the location of the user. This negates the ability to rely on IP data to locate the end-user, through no action or fault of the end-user.
Device-Based Location - Fake Location App (FLA)	A third-party application, (may be unknown to/unapproved by the Apple App Store or Google Play Store) may have the ability to mask the end-user's location. The use of such an application may require obtaining privileged control over an Android or iOS device's sub-system in order to change its system applications and settings. While this is typically done to access device features that may have been blocked by a wireless carrier, it also means that the device's security has been compromised and enables hackers to easily manipulate the end-user's location.
HTML5 Geolocation - Browser Extension	Modern browsers inform websites about a user's location, typically collected via wifi data. Browser extensions allow the user to feed false information into location APIs, allowing them to mask their actual location.
All - Remote Desktop Program (RDP)	An RDP, such as GoToMeeting, has many legitimate uses for allowing people to communicate. However, share screen and remote access features allow users to access content remotely from another device located within the desired location.

GeoGuard actively tracks the most popular and active providers of anonymizer and app-based spoofing services (over 1,000 of them and counting). These companies are agile and market aggressively, often targeting specific content or a OTT broadcaster it knows consumers are looking to watch online. For instance, these companies often target a particular TV series or major sporting league and offer step-by-step guides on how their product can be used to access the same content at drastically lower costs.

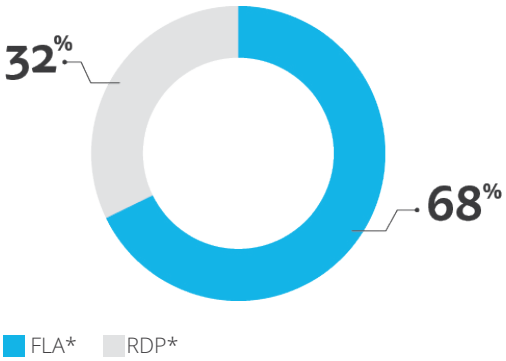
VPNs and other anonymizers are in the mainstream

IP based spoofing:



Source: GeoGuard. n=418

App based spoofing:



Source: GeoGuard. n=678

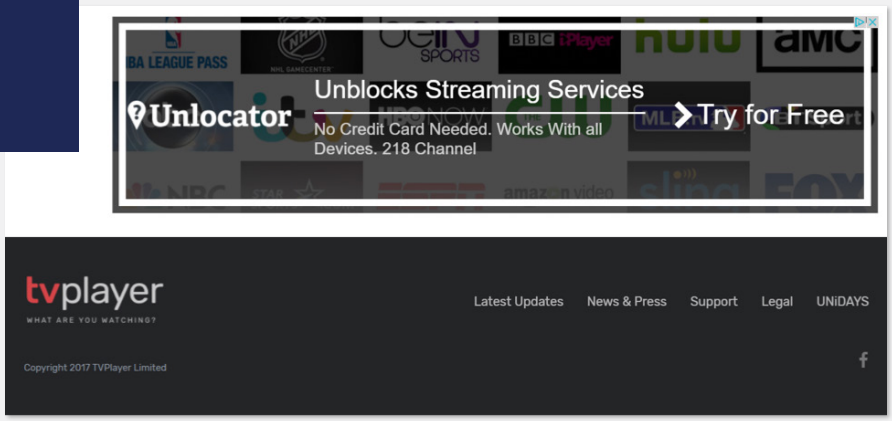
There are more than 250 results for "Fake GPS" on the Google Play store with many apps receiving more than 10 million downloads.

Increasingly, VPN providers are utilizing services which offer access to residential IP addresses, often without the homeowner's knowledge.

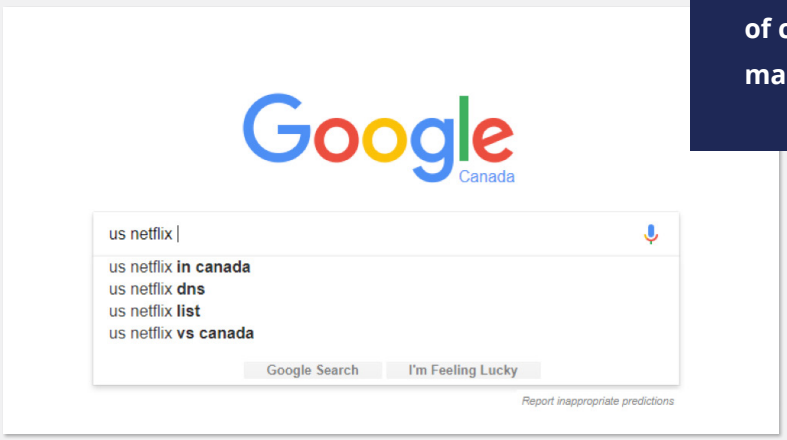
Service	Description
Luminati	Over 19 million residential IPs, 40 GB cost $500/mo. Access to residential IPs enabled via its free Hola!** VPN service
Storm Proxies	70,000 IPs in rotating pool, 10 Threads cost $14
Microleaves	Offering Residential IPs, large P2P proxy network
GeoSurf	Over 2 Million Residential IPs, located In 192 Countries

*Fake Location App (FLA); Remote Desktop Program (RDP).
**Hola! claims 127 million users worldwide while their Google.
Chrome web browser extension alone has over 10 million users.

Unlocator, a Smart DNS service, targeting its ads towards UK streaming service TV Player.



In Canada, Google's search prediction reflects the popularity of consumers searching for grey market access.



Assess What the Industry Standard Should Be for Obtaining End-User Location

In the OTT space IP address-based verification is poorly executed and insufficient due to the growth of device-based location methods - particularly on smart phones, where the IP will always be the location where the phone is registered. Therefore it's more important than ever for rightsholders and broadcasters to employ effective geolocation technologies.

Example of the inefficiency of mobile IP geolocation:

Using a mobile phone located at an office in Vancouver, BC that was connected to the internet via mobile data (LTE) we queried five IP geolocation databases. See the results below:

	City	Latitude	Longitude	Implied accuracy* (meters)	Distance from true location (km)
Vendor 1	Calgary, AB	50.91569	-113.89199	1.1	683.2
Vendor 2	Surrey, BC	49.1889	-122.873	11	21.7
Vendor 3	Vancouver, BC	49.24966	-123.11934	1.1	4.0
Vendor 4	Vancouver, BC	49.245	-123.1337	11	4.4
Vendor 5	Winnipeg, MB	49.24966	-123.11934	1.1	1,866.0

*approximate values at the equator

The results show that not only are these results inaccurate, they often include lat/long coordinates to four or five decimal places, creating a false impression of precision. These fourth and fifth decimals imply accuracy to 11 meters and 1.1 meters respectively - none of the providers are close to this. Due to this issue, even the most respected providers don't recommend using mobile IP addresses for anything other than country level.

Use Case

Scenario 1a – IP-based Geolocation

Whereby geolocation is performed using the end-user's IP address.

Use Case: A sports fan in the United Kingdom wishes to watch English Premier League football matches without paying for a domestic Pay-TV subscription. While undertaking some online research, the sports fan comes across a foreign free-to-air OTT broadcaster which shows the same games in English. However, the website cross-references the fan's IP address against a standard IP location database, detects that it comes from another country and displays an error message stating the location is outside the broadcast territory.

The fan undertakes some additional research and uncovers several VPN providers with webpages detailing ways to circumvent the problem. After signing up to Hola, Mozilla, or a $1-5 per month VPN subscription and installing a small piece of desktop software or browser extension, the IP address can be set to be inside the foreign broadcaster's territory. Upon revisiting the free-to-air website, the website fails to detect the IP address as one that has been used for the last three months by the VPN provider and grants full access to watch the games.

Solution: When the fan visits the OTT broadcaster website via a VPN, their IP address is screened against a highly accurate and up-to-date database of known IP addresses used by IP anonymizing services - this database is updated several times a day*. The IP address is recognized as one belonging to a known data center which hosts VPN connections. An error message is displayed informing the fan that the IP address is outside the broadcast territory.

NOTE. As many VPN/DNS Proxy providers aggressively target major OTT platforms such as BBC, Hulu, Netflix etc, the refresh rate for the database of known IP addresses must be set to several times a day and the OTT site may have to collaborate with the vendor to ensure that defenses are adjusted rapidly enough to keep barriers effective.

Use Case

Scenario 1b – Mobile IP-based Geolocation

Whereby geolocation is performed using the end-user's IP address.

Use Case: A UK expat wishes to watch British programming while living in New York City. The specific TV shows are available for purchase in the US iTunes store however the expat attempts to access a free-to-air OTT app previously used at home in the UK. Connected to wifi, the app detects that the device's IP address originates from Manhattan and denies access.

However, the nature of mobile connections, whereby the IP address is randomly generated by the provider, means that the OTT app is unable to accurately detect where a mobile device is located. By disconnecting from wifi and using a sim card from a UK mobile operator offering free data roaming in the US, the OTT app is unable to establish that the device is not in the UK and grants full access.

Solution: The OTT broadcaster should implement logic on its server so that in the case where a mobile ISP is detected and therefore the IP data is not trusted, then the OTT server should request other types of data, such as wifi or GPS. If these additional sources are not available, the user should be prompted to enable location services in order to access content.

Use Case

Scenario 2 – Device-based location

Whereby geolocation is performed using functionality native to the end-user's device, e.g. GPS or wifi.

Use Case: A US consumer wants to watch the latest movies in Spanish. The consumer is aware of a streaming service which broadcasts across a number of Latin American countries, that is cheaper than the equivalent options available in the US. Using a tablet connected to a wifi network, the consumer downloads the relevant app in order to sign up to the service. Upon launching, the app queries the tablet's location services and informs the server that the wifi connection is located in Las Vegas, Nevada.

However, the subscriber has two options:

Fake Location App – by visiting the app store on the tablet, the subscriber can download a broad range of fake location apps and set it to report its location as within the domestic broadcast market. Accessing the app again, the streaming service is now successful.

Developer Tools – by switching to a laptop, the subscriber can enter the developer console within the laptop's web browser. With the help of an online guide, the subscriber manually alters the latitude and longitude recorded in the browser to be within the domestic broadcast territory. Accessing the app again, the broadcaster's server is unaware that the data has been manipulated and allows full access.

Solution: By integrating a SDK based solution into the website's JavaScript or streaming app, the broadcaster is able to detect that the location details being received have been altered or that a fake location app has been installed. In addition, specific rules can be set, giving the broadcaster greater control over what criteria needs to be met.

Use Case

Scenario 3 – HTML5 based Geolocation (mobile connection)

Whereby geolocation is performed using functionality native to the end-user's device, e.g. GPS or wifi.

Use Case: A US NBA fan wants to watch the upcoming basketball season. The fan is aware of a streaming service which broadcasts across a number of South East Asian countries via a mobile website. Using a device connected to a mobile internet service, the consumer visits the foreign website. The service is able to attain via the location API that the mobile device originates from a mobile connection in the US and blocks access.

However, the consumer has two options:

Developer Tools – by switching to a laptop, the subscriber can enter the developer console within the device's web browser. With the help of an online guide, the subscriber manually alters the latitude and longitude recorded in the browser to be within the target broadcast territory. After disabling wifi and location services, the fan visits the website again and the broadcaster's server is unaware that the data has been manipulated and/or is unable to verify GPS/wifi location, and grants full access.

Browser Extensions – By searching for solutions online, the fan discovers and downloads one of a number of HTML5 browser add-ons which allow the fan to alter the information the mobile browser delivers to the location API. Returning to the mobile website, the streaming service is now successful.

Solution: By integrating a SDK based solution into the mobile website's JavaScript, the broadcaster is able to detect that the location details being received have been altered or that a fake location app has been installed. In addition, specific rules can be set giving the broadcaster greater control over what criteria needs to be met. For instance, if GPS or wifi data is unavailable, the website can prompt the user to enable additional services before granting access.

Recommended Steps

OTT broadcasters need to implement a high standard of end-user location verification to ensure they remain compliant with rightsholders and protect their own business and pricing models. To achieve this, broadcasters need to ensure their product and third-party vendors cover the following points:

Verifying that users are in a permitted location based on IP-geofiltering

- Ensure that a reputable VPN/Proxy detection vendor is used that has been INDEPENDENTLY TESTED AND APPROVED by a 3rd PARTY (such as Cartesian and Kingsmead) as having strong defences against both VPNs and DNS Proxies.
- Ensure that logic is applied to recognize cellular connections (e.g. 3G, 4G, LTE, 5G etc) and IS NOT USING IP GEO-FILTERING LOGIC on such connections but is instead pushing for ALTERNATIVE LOCATION VERIFICATION methods such as HTML5 geolocation and/or device based location methods including wifi, GSM triangulation and/or GPS.
    - Be aware of the challenges faced with IPv6 and it's growing adoption amongst internet users. Not actively tracking IPv6 addresses, will leave premium content unprotected and open to geolocation fraud and geo-piracy.

Verifying that users are in a permitted location based on device-based location data

- Ensure that sufficient tools are employed to provide all necessary defences against FLAs and 'developer Tools' for location spoofing. Proper qualification that these services are adequate could come in the form of taking a SDK or API from a vendor that has undergone independent 3rd party testing ensuring their service offers STRONG defences against this kind of spoofing.

Verifying that users are in a permitted location based on HTML5-based location data

- If HTML5 based geolocation is used, ensure that a qualified 3rd Party JS SDK or API is used which includes all necessary defences against Location Spoofing Extensions and 'developer tools' for location spoofing. Proper qualification requires the vendor has undergone independent 3rd party testing that their service offers STRONG defences against this kind of spoofing.

How GeoGuard Can Help

At GeoGuard, we focus solely on geolocation-based security and protection of digital content. As the independently rated market leader for protection against VPNs and DNS Proxies, we help the OTT ecosystem stop geo-piracy and ensure rightsholders are receiving the full value for their content. For example, **prior to implementing GeoGuard, we identified up to 70% of connections to one of our customer's OTT sites as coming from VPNs.**

GeoGuard provides a suite of geo-filtering solutions combined with human intelligence to stop internet users spoofing their location. GeoGuard's solutions are based on the award-winning geolocation and geo-protection technologies that its parent company GeoComply developed for the highly-regulated and complex digital gaming industry.

Our software is installed in over 300 million devices worldwide, putting GeoGuard in a uniquely powerful position to identify and counter both the current and newly emerging geolocation fraud threats.

Contact us to learn more at solutions@geoguard.com | geoguard.com

GeoGuard is also available through Akamai and AWS Marketplace

GEOGUARD

Fraud Has No Place To Hide