WINTER 2016 $25

M&E JOURNAL

Media & Entertainment Strategies. Solutions.

Special Issue: Security Solutions

How M&E companies are protecting their content with new technologies.

New Workflows

Optimizing Workflows for Digital Success P. 34

Cloud Creation

Capacity and Innovation Meet in the Cloud P. 60

Data Driven

The Data Possibilities of New Delivery Platforms P. 80

Smart Content

Improving Consumer Experience with Smart Content P. 88

PLUS: VR, 4K Ultra HD, Cord-Cutting, Cross-Screen and More

published by MESA
Media & Entertainment Services Alliance

Controlling Content Access in a Borderless (Internet) World

Service providers are getting smarter about geo-filtering for internet-savvy consumers

By Tom Thomas, Senior Consultant, Cartesian

Abstract: Massive improvements in access, speed, and quality have given meteoric rise to internet-delivered content over the last few years. Owners and distributors of content have licensing agreements largely based on geographic boundaries; consumer appetite for content, however, is borderless. The combination of OTT content platforms and the existence of cross-border online pathways, such as VPN, facilitate access to content worldwide, making content distribution more difficult to monitor, safeguard, and ultimately, control. This article delves into the challenge that content owners and distributors are facing to meet their licensing and distribution agreements and what can be done about it.

The last few years have seen a steep rise in the consumption of internet-delivered, or streamed, content versus traditional television. This change, along with recent technical innovations, is causing disruption of a fundamental pillar of the content owners' license model: the control of content release windows on a country-by-country basis via content distributor partners. Online service providers (Over-the-Top players), apply geo-filtering and other mechanisms in their services to restrict content access. In response, consumers use geo-circumvention methods to bypass restrictions. Whenever a popular circumvention route is blocked, a new one pops up to take over. Netflix referred to this situation as a "cat-and-mouse game." Will it ever end?

It is typical for content owners to license material to service providers (SPs) with strict territorial restrictions regarding access. Service providers, in turn, detail geographic usage restrictions in their Terms of Service (ToS) with customers. Mechanisms to restrict access to their content library are deployed by SPs to enforce their license obligations. In the case of an SP serving a single country, for

The practice of geo-circumvention detection gives SPs options for control beyond simple blocking of users. There is the opportunity to steer users towards legitimate routes to the desired content.

example, attempts to play content elsewhere should fail, with a message presented to the user. Other SPs, such as Netflix and Amazon, which have multi-geography presence, will present content catalogs tailored to location in addition to applying technical mechanisms to control access.

Geo-detection: How it works

In order to determine a user's location, most SPs analyse the IP address of the device attempting to access the service. The SP may query the IP address as part of every request the user makes to its website or Content Distribution Network (CDN). These requests include login, browsing, title selection, and queries at various playback points. This IP address is then compared against a geo-location database to determine from which location the attempt to play is coming. There are several third party geo-location databases available.

It is widely known that the U.S. Netflix catalog has significantly more content titles than any of Netflix's other national libraries. This has resulted in a significant number of its Canadian subscribers using circumvention mechanisms as a way of gaining access to the content they can't find at home. This is an example of the content access battle. Whether consumers are aware of, or understand, the restrictions in their ToS, or have a laissez-faire attitude towards content, when faced with a content block many users will find alternative means to access the restricted content. This is a particular issue due to the ease with which these methods can be quickly shared – via social media, forums, etc. – and is not merely the preserve of a small clique of specialists.

Geo-circumvention: How it works

There are two primary means of bypassing geo-blocking technologies. The first, a Virtual Private Network (VPN), allows a private tunnel to be formed between the user's device and a remote server. The remote server is in the target country and presents a public (internet facing) IP address in that location. VPN services vary in their breadth - for example, the number of devices that may be used, monthly download limits, choice of endpoint servers, etc. Services with payment plans that are based on volume of data may become problematic for users consuming large amounts of high-bandwidth video.

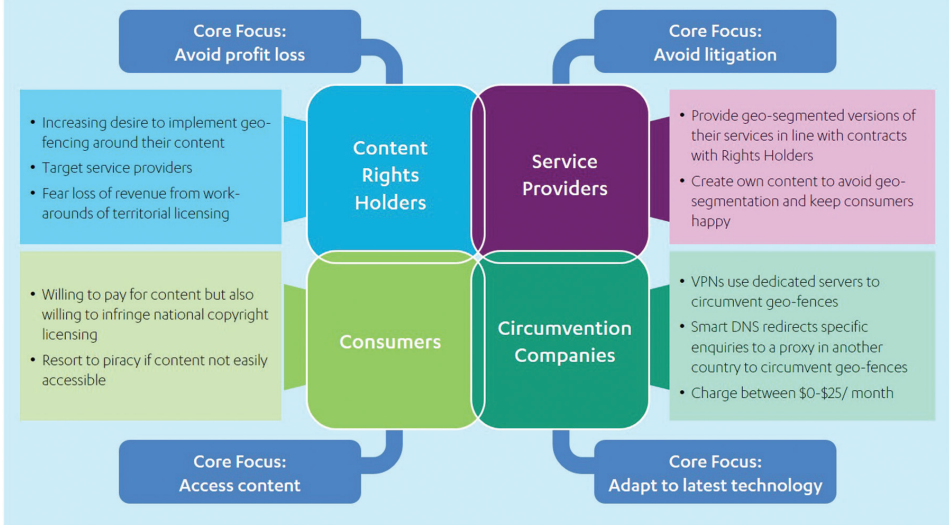
The second approach, a Domain Name System (DNS) proxy, is generally aimed at users wishing to perform geo-circumvention of video streaming sites rather than internet privacy. Unlike VPNs, there is no inherent privacy in a DNS proxied connection. DNS proxies sit between the user and SP filtering specific HTTP requests that are destined for that SP, whilst leaving other general internet traffic untouched. The filtered requests are rerouted via a proxy server within the target country that presents a local IP address to the SP. These simple DNS proxy mechanisms may be free or paid for, but are generally cheaper than a VPN mechanism. As an added advantage for the user, DNS proxies may be setup on a user's home router, which would allow all devices on the home network to take advantage of the mechanism without having to intervene on each device.

The majority of VPNs and DNS proxies are application based, but the most convenient mechanisms are browser plugins. Although convenient, they will only work with browser-based services.

Geo-blocking: SPs strike back

Until early 2016, some SPs were reticent on the topic of blocking, and especially on penalizing users who flouted their ToS. Indeed, to go down this road, there must be robust evidence that a user is deliberately seeking to

The Four Domains in the Conflict for Content Protection and Access



Sources: Cartesian, Smart DNS Proxy, That One Privacy Site

This graphic highlights the conflict between the interests of consumers and content creators, the pressure on service providers, and the innovation drive of 'circumvention companies'.

Tom Thomas is a security expert in the digital TV space with detailed knowledge of CA and DRM systems and their implementations on contemporary STBs and other platforms. At Cartesian, he provides commercial and technical advice to clients, and conducts the Farncombe Security Audit on digital media content systems.

change their perceived location – implying that the SP can only restrict users who it knows with surety are attempting to perform geo-circumvention. Any action on geo-enforcement was also likely to upset some of its customers.

However, whether it was because of pressure from content rights owners and the threat of litigation, the availability of new detection methods, third party firms starting to offer detection as a service, or a combination of these, SPs have been improving enforcement. For example, in line with its launch into 130 new countries at the start of 2016, Netflix, the leader of multi-geography OTT streaming, tightened up its ToS and geo-enforcement measures.

Ultimately, the SP is in the best position to develop a holistic geo-enforcement solution, as only the SP is privy to logs containing both IP address and user account details. Geo-circumvention is detected by comparing a user's IP address against a database of known IP addresses that originate from circumvention mechanisms. Detection techniques are generally a combination of manual spot-checking and automated intelligence gathering. For example, a big data analysis could reveal that accounts that are consistently appearing to be located at the same range of IP addresses, which could be due to the use of a proxy.

Geo-location companies continually monitor and track the ever evolving circumvention providers as they move or add new IP addresses. However, this is not an easy exercise. VPN providers will seek to go the extra mile in order to stay undetected as providing client privacy is their raison d'être. Also, in response to detection and geo-enforcement actions, popular geo-circumvention vendors actively keep their user base abreast of when the latest round of geo-blocking has been re-bypassed. This ongoing pursuit and evasion of circumvention mechanisms has been referred to as a constant game of cat-and-mouse. Still, there are signals of the start of a turning tide: uFlix, a popular unblocking vendor for the Australian market, announced in August that it was going to "stop supporting Netflix as an unblocked channel," citing unaffordable time and resources required. This is the first known public admission of a vendor admitting defeat.

The future of geo-filtering

The practice of geo-circumvention detection gives SPs options for control beyond simple blocking of users. There is the opportunity to steer users towards legitimate routes to the desired content. With the triplet of data available to the SP — account ID, geo-location, and content ID requested — much can be learned about user behavior and this information used to inform the business model going forward.

The more drastic option is account termination of users who repeatedly breach the ToS by using geo-circumvention mechanisms. While for the SP this means a lost customer, for the content owner this approach risks driving users towards other means of accessing the content, such as via P2P torrent sites and other forms of piracy.

With the VPN/DNS proxy market predicted to continue to grow, it is clear that this cat-and-mouse game of geo-filtering and circumvention will continue for the foreseeable future. SPs must keep evolving their technical and management solutions to meet the ingenuity of new circumvention mechanisms. Though with improved detection technology and analytics, they are catching up - giving better assurance that the content rights agreements between the service provider and owner are being upheld. ■