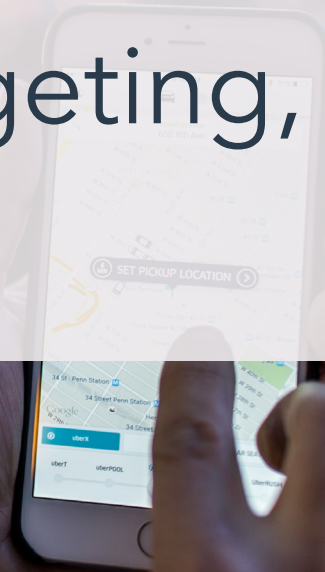




Geo-targeting, Technology Targeting, and Cloaking

FAQ









Most internet users are familiar with how services such as search engines and business directory services use geo-targeting to deliver the most relevant content to users based on their locations. For instance, people searching for pizza online likely want search results near where they live. Geo-targeting is therefore extremely useful in search engine optimization (SEO).

However, illicit operators also use techniques similar to geo-targeting to evade enforcement and hide their illicit activity from internet companies and payment service providers. In this FAQ, we answer common questions about what geo-targeting and technology targeting are, and how they are sometimes used in ways that can put you at risk.



Geo-targeting and More

Frequently Asked Questions

-  1 What are geo-targeting, technology targeting, and cloaking? 4
-  2 What are legitimate uses of geo-targeting and technology targeting? 6
-  3 What are illegitimate uses of geo-targeting and technology targeting? 10
-  4 What do website operators use cloaking for? 15
-  5 How are geo-targeting, technology targeting, and cloaking implemented? 17
-  6 Case Study: An IP-infringing Streaming Website 19

1

What are geo-targeting, technology targeting, and cloaking?

Geo-targeting and technology targeting are useful tools that enhance the browsing experience, typically based on characteristics of the user.

- **Geo-targeting** refers to the method of delivering different content to consumers based on their geographic locations.
- **Technology targeting**, or user-agent targeting, targets users based on their specific browsers, operating systems, or devices.
- Finally, **cloaking** is the method of delivering different content or URLs to human users and search engines.



Did You Know?

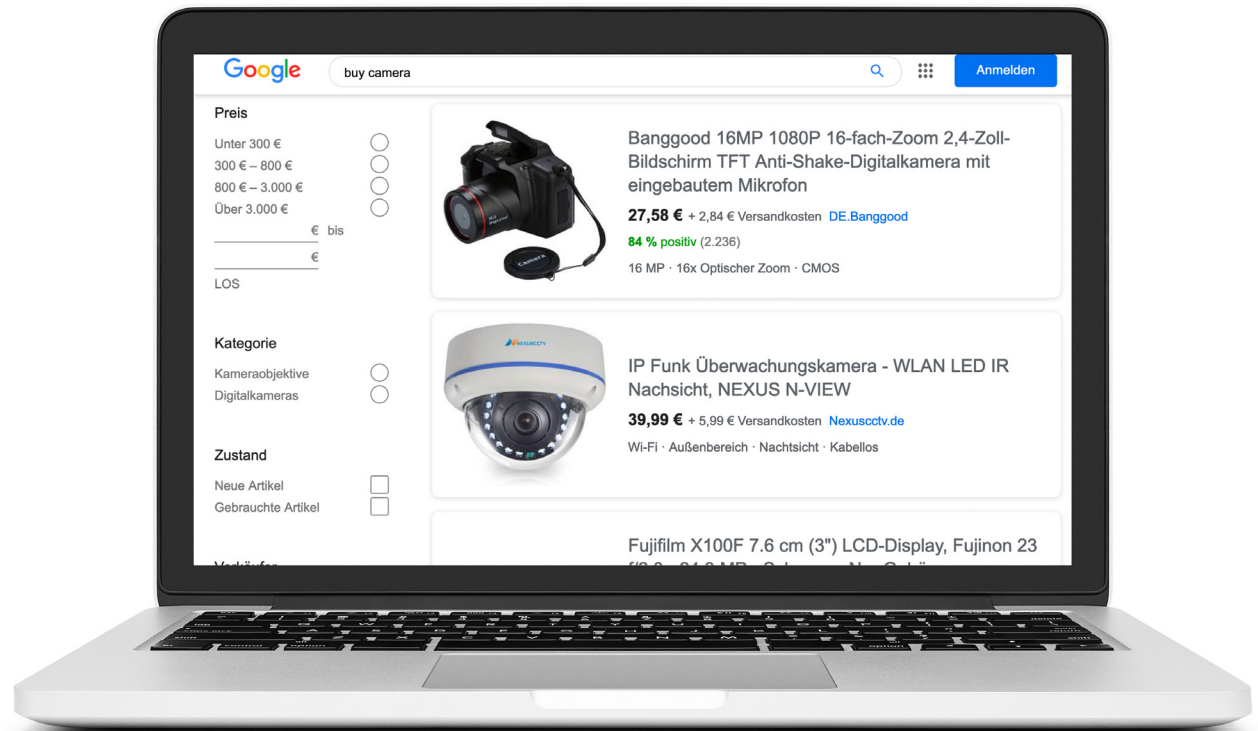
Most search engines, such as [Google Ads](#), offer advertisers tools that allow them to target ads precisely based on user location. An ad can show as broadly or as specifically as an advertiser wants: countries, areas within a country, a radius around a location, or location groups, which can include places of interest, business locations, and tiered demographics.

2

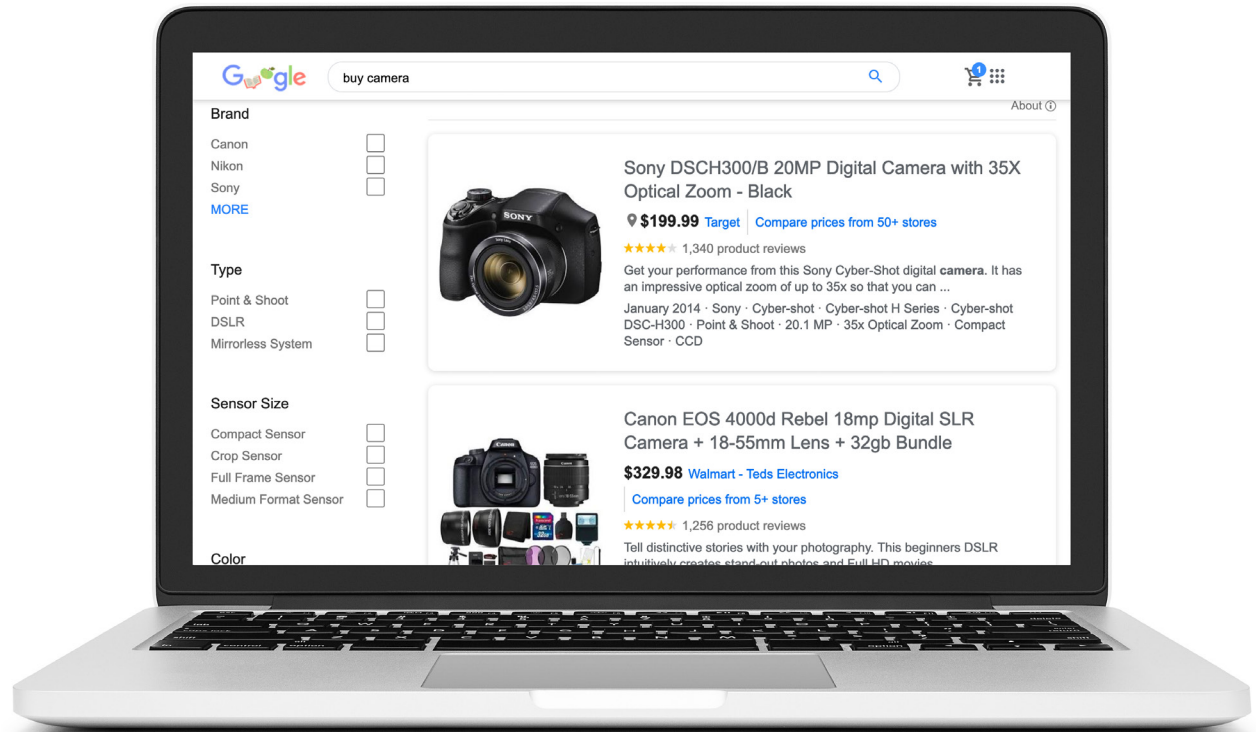
What are legitimate uses of geo-targeting and technology targeting?

Almost anyone operating online — from local businesses, internet search platforms, websites, and phone apps — use geo-targeting and technology targeting to deliver what they believe is the **most relevant data to users** based on their locations and demographics. For example, to maximize user experience and ease, a website can display different languages and currencies based on visitors' geographic locations.

Below you can see how Google Shopping delivers different content and currencies to visitors from different geographic locations for the same search term “buy camera.”



From Germany, Google Shopping displays content in German and currencies in Euros.



For the same search term, when users visit from the US, Google Shopping shows content in English and displays US dollars, plus slightly different products based on shipping availability.

Geo-targeting can also be used to manage intellectual property content. One of the classic examples of such intellectual property content is streaming television. Due to licensing rights, services such as Hulu and Netflix may not provide streaming services, or only provide certain content, to customers outside of the US.

Online websites selling products that might be restricted or prohibited in certain countries may also use location detection to restrict shipping based on a visitor's geographic location. Websites may also geo-target and display different results based on the availability of shipping locations.

Did You Know?

Geo-targeting is an important search engine optimization strategy for businesses trying to rank for the most relevant keywords for their niche, especially in highly competitive markets. Some companies offer multi-regional and multilingual versions of their websites to better target their audiences.

3

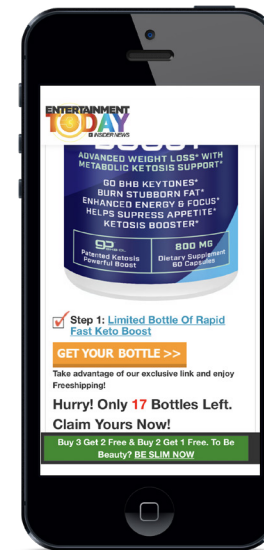
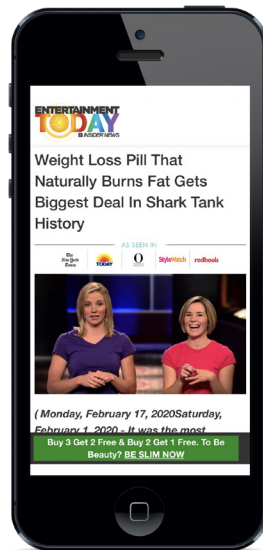
What are illegitimate uses of geo-targeting and technology targeting?

Bad actors can also use geo-targeting and technology targeting to evade enforcement. Websites engaging in questionable or even illicit behaviors may only show **high-risk content** to visitors in certain geographic locations or users with specific device types, while showing innocuous content to visitors from another specific geographic location or using another device type.

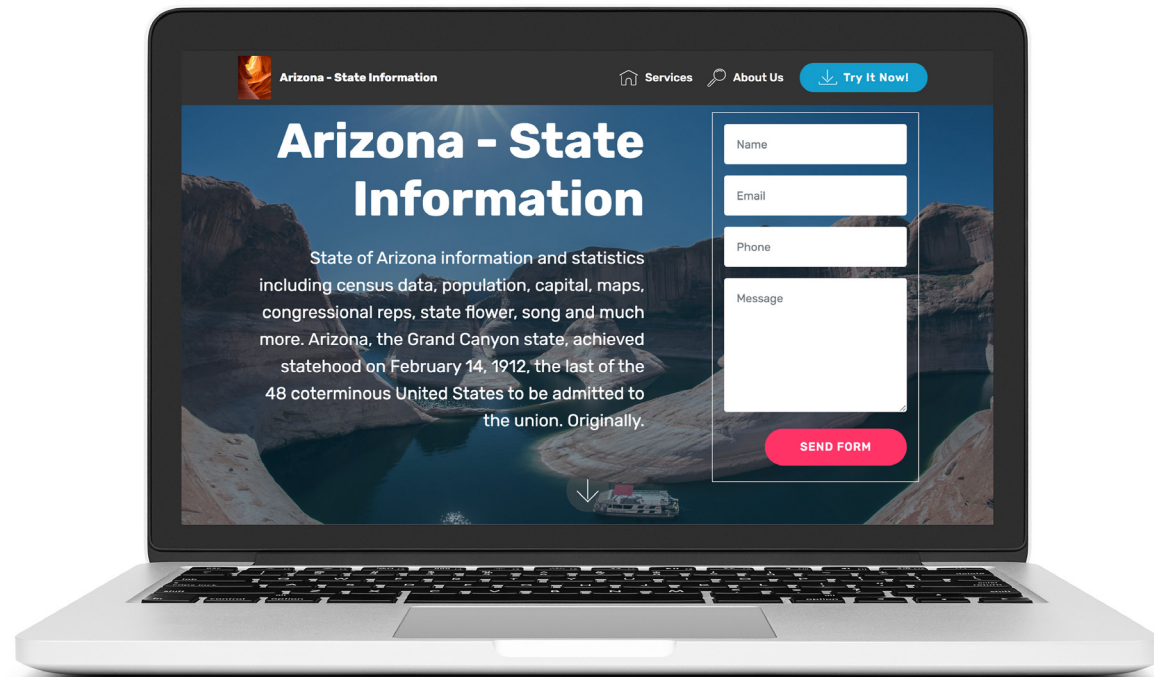
For example, the now-defunct website zh-jhjs.com, shown below, appeared to be a legitimate packaging supplier on a desktop browser (although sharp eyes will notice the IP-infringing Alibaba logo at top).



On a mobile device, however, the website showed **fake news content** marketing high-risk supplements. The website pretended to be a legitimate news website and even featured celebrities who likely did not endorse the products being sold. The “news” content is lathered with outrageously misleading weight loss claims such as “30 lbs of stomach fat loss in just 1 month.” Similar marketing tactics have been cited by the FTC as deceptive.



Another example is the now-defunct arizona19.club, which appeared to be a website showing generic information about the state of Arizona to crawlers.



However, LegitScript was able to detect that the website redirected to a rogue pharmacy website belonging to the PharmEmpire network.



Did You Know?

Some supplement sellers engaged in geo-targeting or technology targeting are also engaged in high-risk behaviors such as negative-option billing. The FTC has warned the public to watch out for these internet marketers.

4

What do website operators use cloaking for?

Cloaking — a controversial practice that is sometimes called “transaction laundering of the advertising space” — is typically considered a form of “black hat” SEO. In fact, cloaking is considered a **violation of many search engines’ and social media platforms’ policies** because it can serve users with different results than they expected. Furthermore, in many cases, cloaking can also be used to affect search engine rankings by fooling the search engine’s algorithm. Illicit advertisers engaging in questionable behaviors may also use cloaking to **evade detection** by crawlers and/or ad reviewers.

When a website is hijacked, the hijackers can also use cloaking to make it more difficult for the primary website operator to detect the intrusion. Violative content may only show in particular instances. This can make it difficult for search engines to catch and enforce hijacked content.

Did You Know?

To help cut down on spam and potentially violative content, cloaking violates the terms and conditions of [Google](#), [Facebook](#), and [Bing](#).

5

How are geo-targeting, technology targeting, and cloaking implemented?

Geo-targeting, technology targeting, and cloaking can have similar but different methods. A geolocation can be detected via a website visitor's IP address, device ID, GPS signals, and more. Some of the methods cloakers can use may include:

- Collecting and recording IP addresses that visit the page, and blocking questionable ones
- Detecting a visitor's referral URL and/or user agent HTTP header and blocking ones that look as if they might be coming from a content reviewer or a crawler

- Banning or showing different content to visitors in a specific geographic location where content reviewers or enforcement agencies may be located

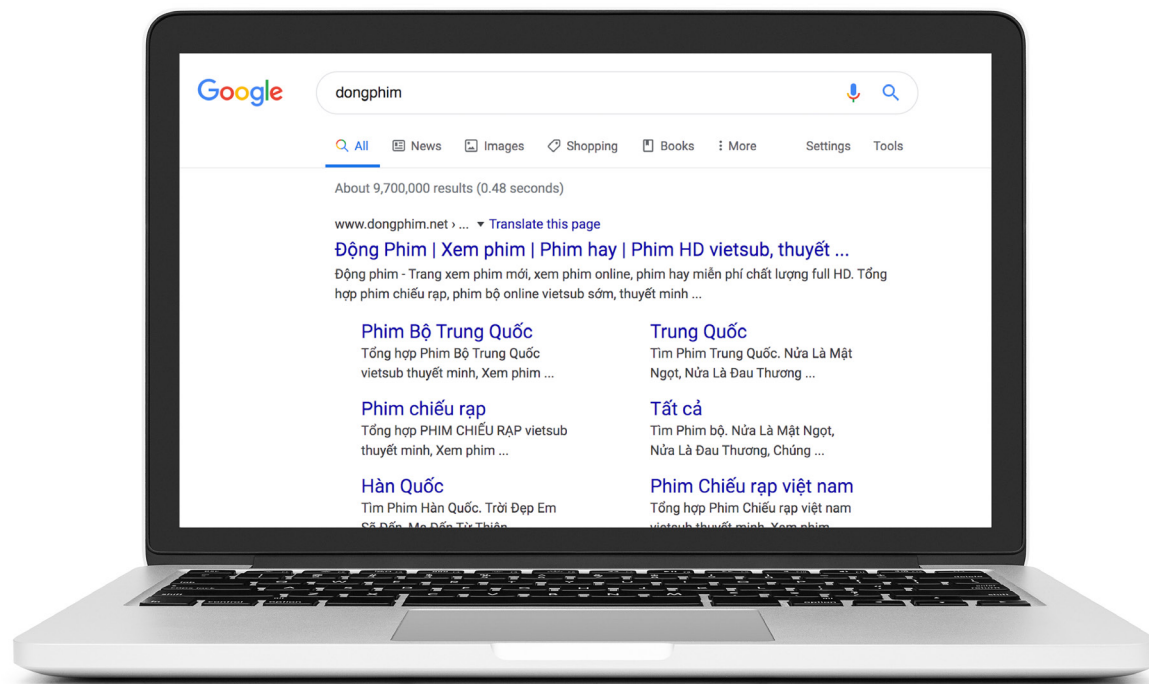
Oftentimes, these websites **utilize scripts** such as PHP scripts, which are the components embedded in HTML codes, to make their websites behave dynamically, including delivering different content to different users.



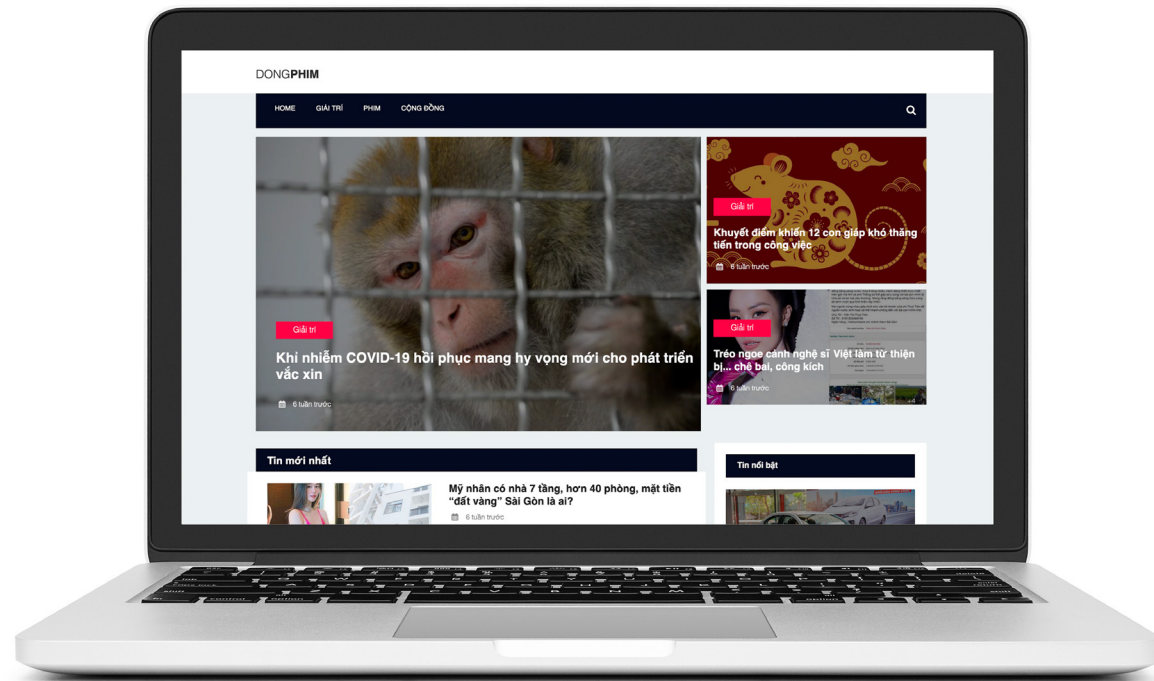
Case Study: An IP-infringing Streaming Website

dongphim.net is a website that allows visitors from specific locations outside of the US to illicitly watch **copyrighted videos for free**. However, to avoid detection from copyright holders and enforcement agencies, it cloaks itself as a news website to users based in the US, where enforcement is strongest.

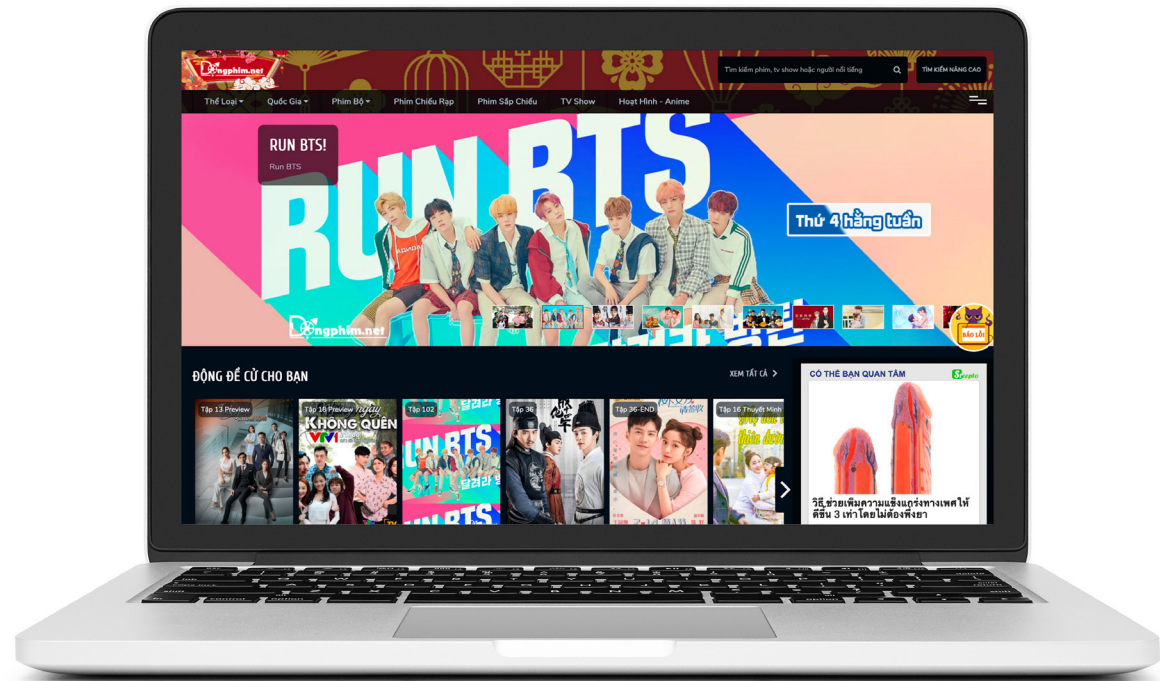
Searching for its domain name via Google shows that the website title is “Động Phim | Xem phim | Phim hay | Phim HD vietsub ...,” which translates to “Movie Cave | Watch movies | Good movies | HD Movies vietsub”



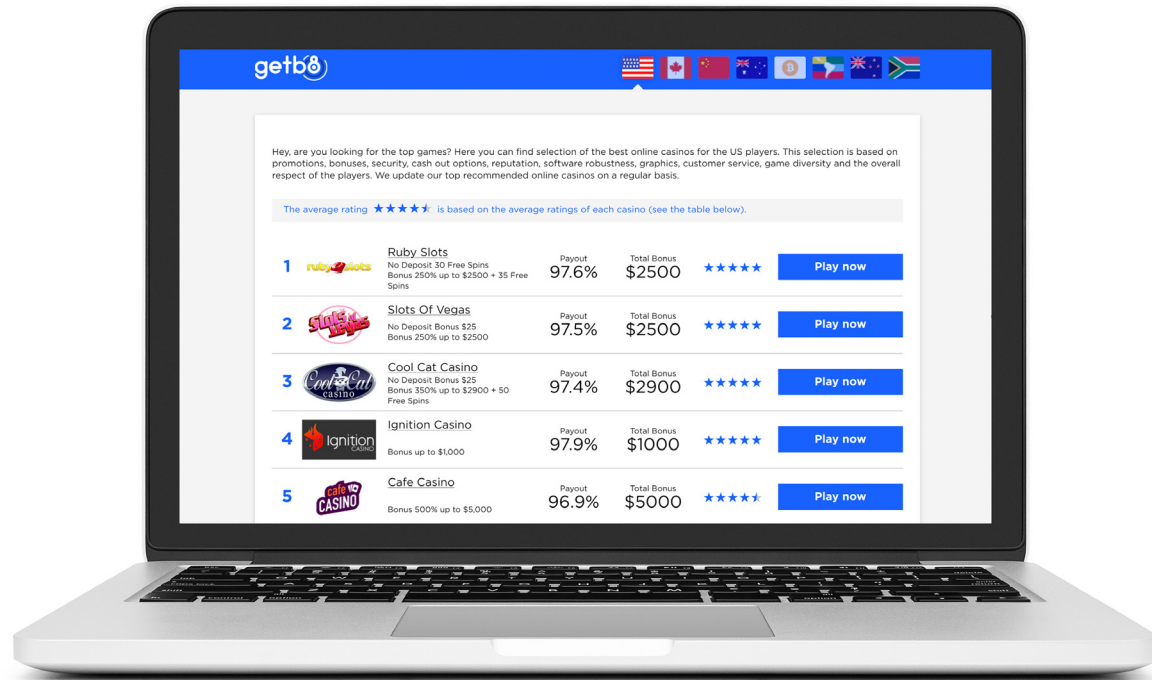
For users located in the US, the page typically takes a few seconds to load as a geo-targeting PHP script appears to be determining which content to show visitors. After the script determines that a user is based in the US, it displays news content, such as the page shown below.



However, visitors from many non-US countries would see a movie page, as shown below. Movies available include a number from Disney, such as Frozen 2 and Captain Marvel, and other titles from common US targets of IP infringement.



Furthermore, the website also displays spammy ads and videos that promote other problematic websites, such as a gambling aggregator platform.



While geo-targeting and technology targeting can be a tremendously useful tool for virtually any legitimate business operating online, these techniques can also be used by illicit cloakers to thrive in internet and payment ecosystems. LegitScript has seen an **increase in problematic advertisers** developing and employing various black hat methodologies, such as cloaking, in order to evade detection. Partnering with a monitoring provider like LegitScript can help you weed out bad actors and the reduce risk of violative content occurring on your platform or in your portfolio.



About LegitScript

At LegitScript, our mission is to make the internet and payment ecosystems safer and more transparent for businesses and the public.

LegitScript experts proactively monitor black hat techniques that illicit operators use to target specific users and evade detection. Our monitoring services provide best-in-class solutions for identifying high-risk merchants and helping our clients remove problematic vendors from their platforms and portfolios.

Contact Us

Phone: 1-877-534-4879

Web: legitscript.com/contact

Keep Up to Date

Newsletter: legitscript.com/newsletter

Blog: legitscript.com/blog

Twitter: [@legitscript](https://twitter.com/legitscript)

You may also be interested in:

The Rise of Website Hijacking



Contact us to get your copy.
