

Domain Blocking for Brand Protection



An Introduction to **Domain Blocking**



Domain Blocking is the practice of blocking your brand or trademark name from registration across a multitude of TLD spaces without actively registering any of the domains. The goal is to protect your trademark from third party or malicious domain registrations

In 2011, ICANN allocated the new gTLD .xxx. In response, the concept of “domain blocking” was created so that brand owners maintained a clear opportunity to protect their name(s) where the risk of brand infringement was evident.

An Introduction to Domain Blocking

A purely defensive measure for brand and trademark managers, domain blocking ensures the most coverage of their marks across hundreds of TLDs — without the tedious need to register each domain individually.

Domain blocking also offers holders the ability to utilize those domain names when needed, turning them into live domains without the risk of open, third party registration.

Generally, domain blocking is more economical than proceeding with a full offensive registration strategy, where domains containing trademarks and names are actively registered as a preventative measure.

In this white paper, we'll discuss the topic of "Brand Blocking" through the lens of domain blocking: how it's evolved from 2011 to 2024, differences between gTLD and ccTLD blocking, new and emerging technologies, and when domain

blocking or defensive registration is the better option for your domain management strategy.

Evolution of Domain Blocking

The concept of domain blocking originated in 2011 as a response to the .xxx gTLD allocation. After being applied for in 2004, .xxx was delegated until 2011 due to controversy around its subject matter.

Why? Because some potential registrants worried about being associated with adult content, so the .xxx registry came up with an innovative solution and domain blocking was born.

It gave brand owners the opportunity to block their names in a space many don't have a market for, and especially so that third parties couldn't register their names in those spaces.

The Evolution of Domain Blocking

“

The most important factor in survival is neither intelligence nor strength but adaptability.

-Charles Darwin

”

We'll try and keep the history lesson brief; Darwin's quote is tied to species evolution, but it could also apply to domain blocking.

Domain blocking evolved from a single TLD block in 2011 to a multi TLD and extension block in 2014 when Identity Digital (formerly Donuts) created the DPML block service. This service, which has since grown to cover over 300 TLDs and extensions, was revolutionary. It gave brand and trademark managers the ability to protect their brand(s) from active registration across a multitude of TLDs and extensions without having to manage a large portfolio, or incur

the costs that are typically associated with that approach. Though initially unpopular, brand and trademark managers came to recognize domain blocking as the positive method for protecting their brands that it is.

Let's skip to 2018 when the Trademark Clearinghouse (TMCH) created the now defunct Trademark Registry Exchange (TREx) block. This block allowed brand and trademark owners to not only block their names in gTLDs, but also ccTLDs (notably, Germany's .de, which is one of the most popular ccTLDs in terms of registration count).

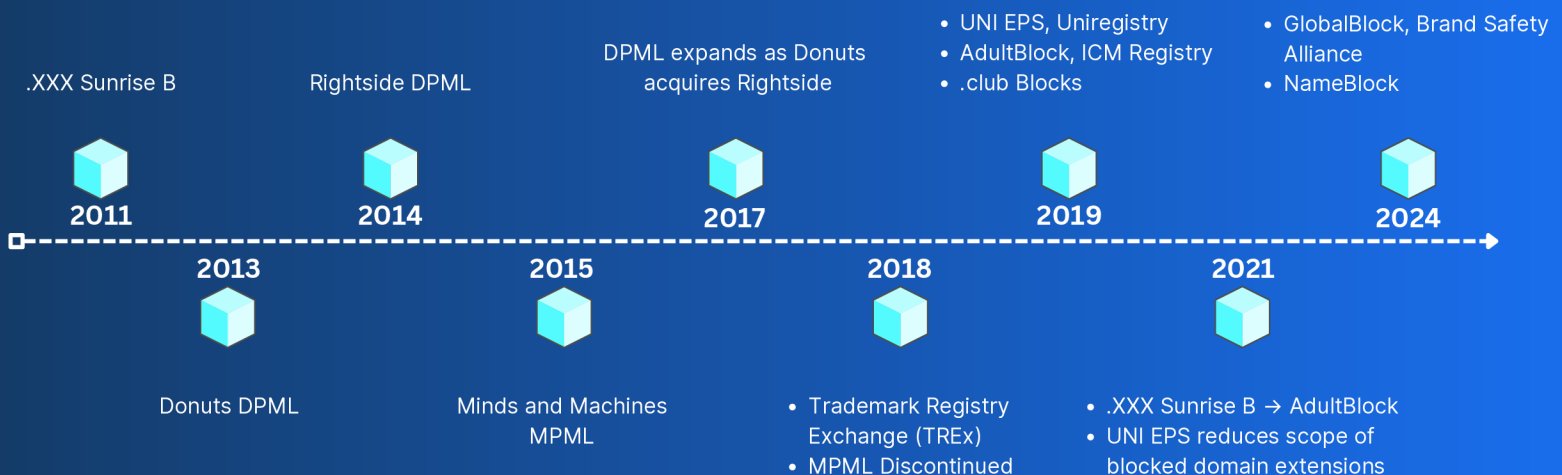
The concept of including ccTLD coverage in domain blocking services was a new idea that gained plenty of traction and has continued to evolve into the offerings we see today.

2024 saw the creation and implementation of GlobalBlock, a

The Evolution of Domain Blocking

service from the Brand Safety Alliance that grants brand and trademark owners the ability to block their marks in over 550 TLDs and extensions, both gTLDs and ccTLDs. They collaborate with the many registry providers who operate those gTLDs and ccTLDs.

Thinking back to where it all started, and now looking at the timeline below, domain blocking has been on track to deliver us with the services of today: valuable, straightforward approaches to online brand protection.



New gTLDs, ccTLDs and Domain Blocking

Now, let's take a look at where blocking fits into the new gTLD and ccTLD landscapes.

History of New gTLDs

In 2012, when ICANN opened the first round of its New Generic Top-Level Domains Program, it set out to enable the continued expansion of the Domain Name System (DNS) — fostering diversity, encouraging competition, and enhancing the utility of the DNS through the introduction of new gTLDs. In the 2012 round of new gTLDs, more than 1,200 new gTLDs were added to the DNS.

History of ccTLDs

Country Code Top-Level Domains (ccTLDs) are a bit older than the new gTLDs we see today. The first delegated ccTLD was the .us (United States) ccTLD in 1985, followed by .uk (United Kingdom) that same year, and .il (Israel), with

other countries having ccTLDs delegated to them in the following years. Now, there are approximately 300 different ccTLDs in 2024.

The scope of the DNS is vast, with many opportunities where brand infringement could occur. While in most cases registering a new gTLD is relatively straightforward, ccTLD registration can be a more complex process.

In order to ensure the localization of the TLD, ccTLDs can have many different registration restrictions. For example, that could mean that an entity needs to provide a presence in the country or region, or that they need to utilize a local agent as a proxy entity for managing the domain.

For years, domain blocking was the standard approach for new gTLD management, because

New gTLDs, ccTLDs and Domain Blocking

implementing a database entry in their root zone that blocks the brand label from being registered by a third party is a simple solution for the Registry Operator (RO).

With the introduction of ccTLD coverage in domain blocking services, brand managers have a

broader toolbox to protect their brand, with the ability to turn any blocked ccTLD into a live registration, for example, in case an organization decides to go to market in that country or region and wants to actively leverage and use that domain.



Web3: An Emergent Internet

The decentralized web, or Web3, can seem a bit intimidating, especially considering the boom in NFT domain registrations that's occurred over the past five years.

In 2014, Web3 was dubbed “the new iteration of the internet” by Ethereum co-founder, Gavin Wood. However, this emerging technology did not gain widespread interest until 2021, which has contributed to significant brand infringement in the space.

For all brand owners, ensuring that you're protected in the Web3 and blockchain space is paramount to both protecting your brand name and preparing for possible future use. In five years, Web3 could be the primary way that some large entities reach their consumer bases, or significant portions of their user base.

Building trust with your consumer group in Web3 starting with owning your digital identify, and that means

owning your NFT domains.

Brand Risks in Web3

A word of caution about Web3 — anyone and everyone who wants to can create a Web3 TLD, mint it to a blockchain, and offer second-level registrations from the TLD they've minted. That does not make their TLD inherently valuable.

There are no standard rights protection mechanisms in Web3, so entities should be vetted before diving into the Web3 space.

Fortunately, for Markmonitor clients, we've vetted many Web3 registry operators to determine which ones are trusted entities and worthy of engagement. We leverage our experience and expertise to conduct proper checks, including reviews of any terms and conditions and policy documents, and by engaging with

Web3: An Emergent Internet

executives and c-suite level employees of these companies.

This due diligence ensures our clients are protected, and that Markmonitor continues to provide that extra layer of security for our clients.

NFT Domain Names

Currently, two blocking services

allow for blocking of Web3 extensions, those being GlobalBlock and their partnership with Unstoppable Domains, and NameBlock with their product BrandLock in partnership with Freename, a Web3 domain service.

The addition of Web3 protections allow brand owners to better protect their marks in the emerging space.



Domain Blocking: Benefits of a Defensive Strategy

Domain blocking offers many benefits to brand managers with regard to their domain strategy.

Chiefly among these benefits is pricing, as it is generally more cost-effective to place a block over a certain number of extensions than it is to actively register and renew each domain.

Depending on your brand and trademark protection strategies, expansive domain portfolios can be difficult to manage. Domain blocking simplifies the scope and complexity of domain portfolio management. If a block is in place, that means a fewer number of domains would need to be actively managed and budgeted for, as compared to if the block were not in place.

That said, there is some flexibility if a brand owner finds they need to utilize a blocked domain. Domains can be removed from a block and activated in the DNS. This ability

gives brand owners flexibility and the option to use the domain in the future should they wish to.

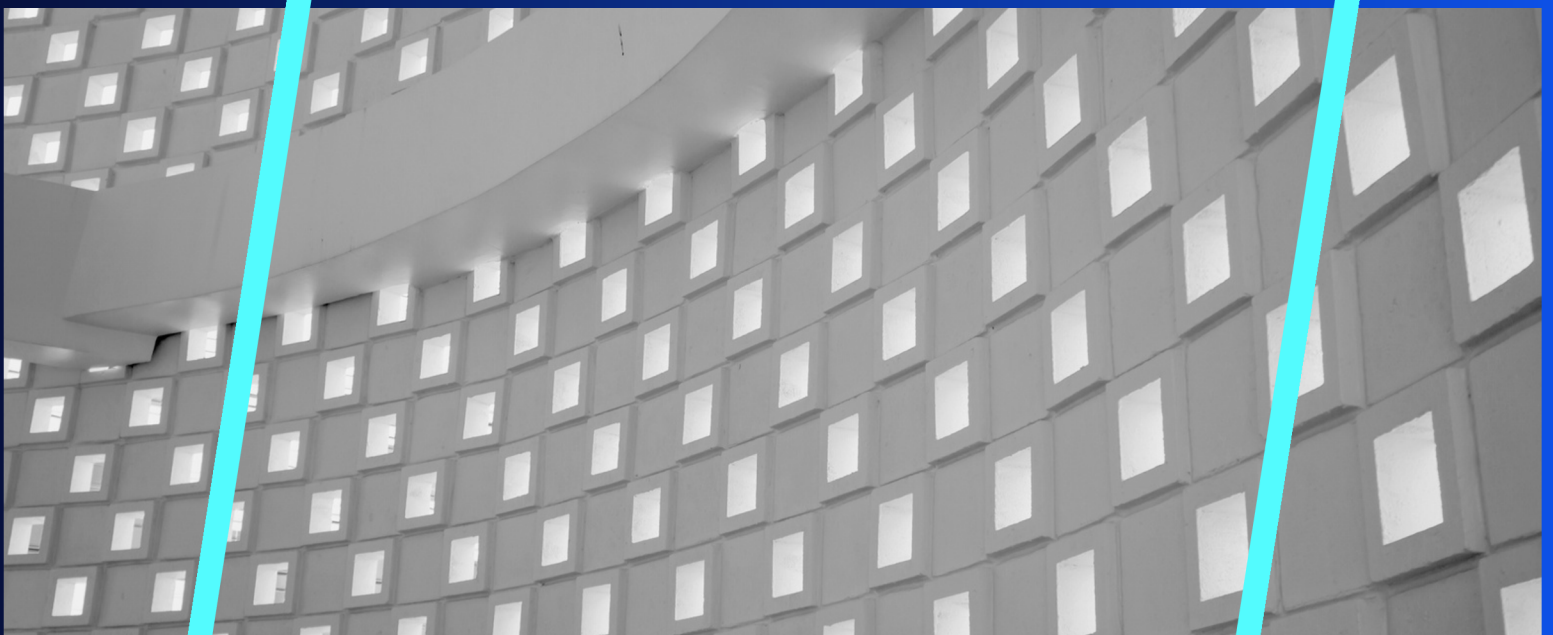
Sometimes, the best approach is the proactive defense strategy: ensure your mark is protected in the domain space before a reactive approach becomes necessary. With domain blocking, instead of reacting to infringements upon your brand name, you can prevent them.

Employing a domain blocking service can be an effective first step in proactively defending your name for brand owners that do not currently have strategies in place for specific domains and TLDs.

Finally, let's revisit a point from a previous section. Restrictions in some TLD requirements can prevent some brand owners from directly registering specific domains, e.g., a ccTLD with local presence requirements.

Domain Blocking: Benefits of a Defensive Strategy

These restrictions can inhibit a brand manager's ability to properly protect their brand name in the digital space. And while those restrictions are in place, they don't prevent every malicious third party from possibly registering your name.



Active Registration or Domain Block?

Should your brand actively register domains or use a domain blocking service as your primary defensive domain portfolio tactic?

If you aren't sure whether you should defensively register your brand name(s) across a wide scope of TLDs or use a domain blocking service, here are some things to consider:

- Don't allow current active registrations to hinder your decision.
 - Many gTLDs are defensively registered by corporations and remain functionally unused.
 - For those domains that are covered by the terms of a blocking service, when the registration expires, they will fall under the block instead of becoming available for third party registration.
- The sale of blocked domains is possible.
 - Having a block in place doesn't prevent your organization from profiting from the domains under the block.
 - Block owners, especially those with more generic trademark names, can unblock domains and sell them to other organizations and investors.
 - For example, if an organization exists that wants to use a .education domain name, but your organization has it covered through GlobalBlock's exact match feature, you could unblock it and a sale and transfer of the .education name could be completed.
 - Selling blocked domains to relevant parties could be commercially profitable

Active Registration or Domain Block?

and a potential partnership opportunity for the organizations.

- What about subdomains?
 - Organizations that utilize subdomains as part of the URL structures for either internal or external facing content cannot have the root domain blocked, it must remain live.
 - For example, if a subdomain like “contactus.markmonitor.info” were in use, it could only continue to be useful and resolve if the root domain “markmonitor.info” remained active.
 - If considering a blocking service, it is a best practice to work with your Markmonitor Account Manager to ensure that all of the subdomains your organization uses won't be affected by the block. By ensuring that the root
- Brand holders beware: When it comes to domain blocking, it's first-come, first-serve, though not all blocks are final.
 - Implementing a block for your brand name across a variety of TLDs does not necessarily prevent other trademark owners with matching trademarks from unblocking a shared mark in specific domains, even if your block is verified as legitimate by your trademark. As long a third party trademark is valid, a domain can be unblocked by that trademark holder.
 - Keep this in mind if your brand has competing marks (perhaps in a different trademark class or jurisdiction). Some may

domain remains active, your subdomains will continue to resolve and be used as normal with the expected results.

Active Registration or Domain Block?

- require approval to unblock, but others do not.
- In most cases, approval and agreement must happen among all parties relevant to the block, other cases have dispute methods in place that may allow a domain you previously protected under a block to now be actively used by the other entity.
- Registry Premium Name Fees
 - In today's gTLD landscape, brand owners are aware that Registry Premium Name fees exist for their matching trademarks, and even for their more generic trademarks.
 - Some blocking services do not cover premium names and if the brand owner's label is deemed premium at the registry, it will not be covered by those blocks.
 - For those looking to have an all-encompassing defensive strategy, active registrations
- will be required to protect your brand.
- Is your brand planning to expand its geographical and digital footprint? Or does it have local markets?
 - When your brand's consumer base is local, or a business entity has plans to expand into a region, the corresponding ccTLDs should not be blocked. Instead, they should be actively used to reach the local consumers.
 - For example, if a brand is looking to expand into the APAC region, securing and actively using a local ccTLD or gTLD could greatly benefit its interactions with its target audiences.

Interested in leveraging **Domain Blocking?**



In this white paper, we've gone through a history lesson on domain blocking, discussed its benefits, and reviewed the new gTLD and ccTLD landscapes with regards to blocking. And we have discussed emerging technologies, such as Web3, and the challenges they can pose for brand owners, along with what considerations a brand owner should make when deciding

between active registrations or domain blocking services.

In the domain space, the challenges of brand infringement and dilution exist — and domain blocking is not a one-stop fix. However, blocking contributes to a strong defensive domain portfolio strategy and should be considered as an effective tool for brand managers.

Should you need any further information or assistance, please contact your Domain Portfolio Advisor (DPA) or email customer.service@markmonitor.com

Markmonitor provides strategic domain management solutions that help protect the revenue and reputation of the world's leading brands.

Since 1999, Markmonitor has served the domain portfolio needs of businesses around the globe, including many of the most visited websites in the world. An ICANN accredited domain registrar since its establishment, Markmonitor leverages its extensive industry relationships, innovative technology, and broad expertise to manage and protect company domain portfolios, all with data-driven, white-glove consultation designed to maximize domain portfolio value.