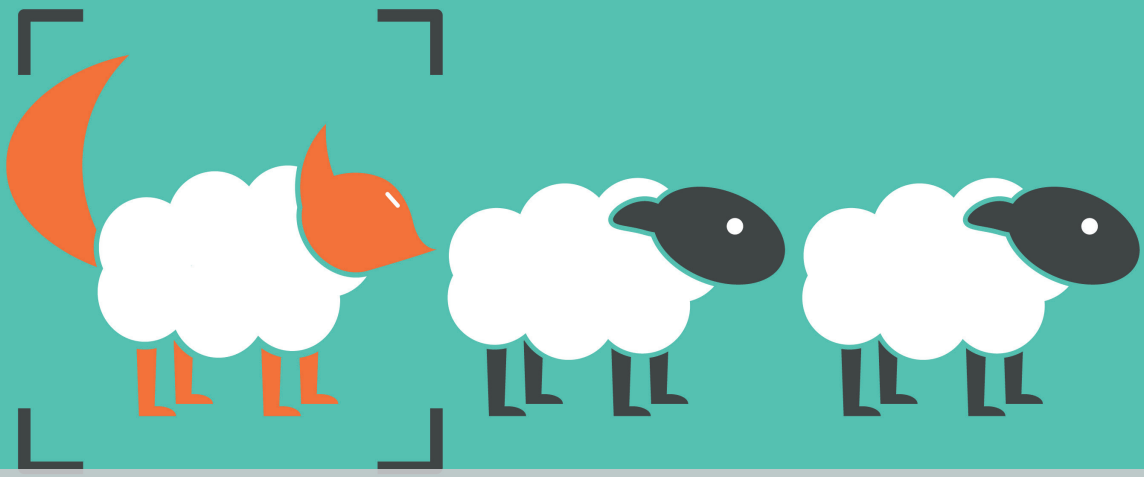
WTR
World Trademark Review

Anti-counterfeiting and Online Brand Enforcement 2021



Industry Insight

CSC

David Barnett

A Global Guide

ACG THE ANTI-COUNTERFEITING GROUP

INTA

ICC INTERNATIONAL CHAMBER OF COMMERCE

Return on investment – proving that protection pays

Author
David Barnett

The implementation of a brand-protection programme can be a costly enterprise for a brand owner. In cases where an external service provider is used, there will generally be monetary costs associated with the monitoring technology and the provision of analyst consultancy that may be required to review results, produce summary reports and carry out enforcement work. However, in addition, stakeholders will need to be appointed within the brand owner's organisation to oversee the programme, collate the prerequisite information necessary for the configuration of the service, and liaise with the service provider to agree on workflows. Significant effort is also often required to ensure that the brand owner's IP portfolio is in good shape and that all associated documentation is available – which is an essential requirement for any associated takedowns. Given the levels of cost and time investment, it is often a requirement for the brand owner to be able to demonstrate to management that the brand-protection service is delivering value, by quantifying the benefits of the programme through a return on investment (ROI) calculation.

Intangible and qualitative benefits of brand protection

In many cases, the process of identifying infringing content on the Internet and implementing its removal through some sort of enforcement – or takedown – action, forms the basis of many standard ROI calculations. However, a brand-protection programme can still deliver benefits even where enforcement is not possible or desirable. One common example is in the identification of negative customer comments or boycott activity. It is frequently the case that content of this type cannot be removed from the Internet, as it is protected by free speech, and even where it may be possible to have the material taken down, it may be unwise to do so for a brand owner wishing not to appear heavy handed in their approach. Even so, having an awareness of this content can still provide value to the brand owner, giving them the opportunity to put out appropriate marketing messaging to counteract the negative 'buzz'.

In its most general terms, the aim of the monitoring components of a brand-protection programme is simply the identification of online references to the brand. Having an understanding of how the brand is being used (and abused) by third parties has value in its own right, even in the absence of an enforcement element to the service. It can raise awareness of issues such as potential brand confusion (the existence of other companies using the same brand name – perhaps legitimately, depending on the product classes and geographical jurisdictions in which IP rights are held) – and brand dilution (where the brand name becomes used as a product descriptor in a generic sense), ideas which are

David Barnett
Subject-matter expert, brand monitoring
david.barnett@cscglobal.com

David Barnett is the brand-monitoring subject-matter expert for CSC, after managing the brand analyst team since 2006. Dr Barnett has worked in the internet brand-protection industry as an analyst and consultant since 2004, helping to serve a range of brand-protection customers in a variety of different industries. He has also presented or contributed to a number of seminars, white papers and press releases, on the subjects of online brand protection, brand prominence and open-source investigation techniques.

key to the idea of brand value. This awareness can help to inform a company's IP protection strategies, product development directions and marketing activities.

For those brand-protection services where enforcement is a key element, it may be possible to qualitatively (or semi-quantitatively) see the benefits of the programme, even in the absence of a formal set of ROI calculations. One simple driver for commissioning a service might be for financial services brands or other organisations where there may be a regulatory requirement the company to have a brand-protection solution in place. Beyond this, one of the top-level aims of a programme of monitoring and enforcement might simply be to see the number of identified egregious findings decrease over time, as infringements become less common and harder to identify online. Potentially, as criminals observe that their content is being taken down, they will instead turn their attention to targeting other organisations that are perhaps not seen to be as proactive at defending their brands and therefore appear more attractive. Some companies may, for example, set themselves the aim that there should ultimately be no infringing content returned on the first page of results returned by a search engine in response to a brand-specific query. This can be achieved through a combination of content takedowns and search-engine delistings.

Even when the observed numbers of infringements appear to be dropping off, it is crucial to continue the monitoring and analysis to ensure that nothing is being missed. For example, if infringers become aware that a brand owner is monitoring and enforcing against brand-specific content, they may resort to techniques such as making use of brand abbreviations or deliberate misspellings – which are obvious to the human eye, but might not be identified using an automated monitoring solution – as a means of evading detection. Similarly, in some cases, infringing products might be described using only generic keywords and with no brand references in the textual components of the listing. A brand-protection solution must therefore incorporate the provision of detailed analysis and intelligence to identify such trends and ensure that the monitoring continues to evolve over time, so that any variations of this type can continue to be captured. In addition, it may be necessary to adapt the enforcement process (see Table 1), depending on the way in which the brand name is being used (or not used).

It is also important to ensure that observed trends are not misinterpreted. It may typically be the case with a brand-protection service that the types of infringement identified change over time for different reasons (eg, changes in focus by the infringers and general online trends). These variations may result in changes to the types of enforcement action (see Table 1) that are typically required, so that a more mature service may, for example, include an emphasis on takedowns that are generally more difficult and time-consuming to carry out – the raw numbers alone do not necessarily provide the full picture.

Quantification of lost and reclaimable revenue: the ROI calculation

Providing that a brand owner has appropriate IP protection in place, there will generally be a range of options available to achieve the removal of infringing content (see Table 1). The overall aims of an ROI analysis are to quantify the revenue losses associated with the existence of this content before its removal, and to determine the proportion of this revenue that can be potentially 'reclaimed' following successful enforcement. The links between infringing content and the associated revenue losses are particularly clear in some cases, such as where fraudulent ('phishing') sites are harvesting user credentials from financial-services customers, thereby providing criminals with direct access to customer funds, or where non-legitimate e-commerce sites are offering the sale of counterfeit products, directing the revenue stream away from the legitimate supply chain.

Domain recovery

The context in which the philosophy of an ROI calculation is most easily understood is in cases of domain acquisition (recovery). This is the process whereby a brand owner can attempt to reclaim a brand-specific domain name that is currently under the ownership of a third party, via an investigation and dispute process. The process can be followed in cases where the domain name contains the brand owner's trademark, the domain qualifies for recovery, and the brand owner wishes to take ownership of the domain name. Success will be dependent on factors such as whether:

- the trademark rights pre-date the creation of the domain name;
- the domain name is confusingly similar to the mark;
- the current owner has rights or legitimate interests in the name; and
- there are any indications of use in bad faith.

If an infringing domain is successfully reclaimed by the brand owner, the web traffic (ie, the daily numbers of visitors) received by the site can be redirected to the brand owner's official site and a proportion of the traffic can therefore be 'converted' to generate revenue for the brand owner. On this basis, it is possible to quantify the ROI associated with the domain monitoring and recovery process. The calculation requires a number of inputs and assumptions. One key piece of data is the amount of traffic received by the site, and numerous online tools and databases are available to provide estimates of this information. Web-traffic data is generally determined by these service providers through a combination of analysis of the browsing

TABLE 1: Examples of enforcement options available for the takedown of infringing content for a range of different online channels

Channel or content type	Enforcement options		
			Escalation
Domain name issues	Cease and desist notice to registrant	→	Notice to host
	Notice to host		
	Notice to registrar		
	Parking page provider deactivation		
	Domain acquisition/recovery process		
e-commerce (marketplaces)	Report directly to marketplace		
Social media	Cease and desist notice to user		
	Report directly to social media site		
Mobile apps	Digital Millennium Copyright Act notice to developer	→	Notice to host (for standalone app-download sites)
	Report directly to app store		

patterns of the provider's customer base, and published webserver data from a wide range of popular sites. In some cases, the data may be provided in a more granular form, giving information on geographical trends or variations over time.

The other assumptions required for the ROI calculation relate to the conversion rate for visitors to the brand owner's official site (ie, the proportion of visitors who make a purchase or become a customer) and the average value (or spend) of these customers. These assumptions can be adjusted based on input from the brand owner and may make use of information such as the company's own website analytics and financial performance and sales volumes (Table 2 illustrates how the components of the ROI calculation fit together in practice).

A similar approach can be used to quantify the ROI associated with other types of domain enforcement action, even in cases where the domain is not recovered by the brand owner (and it is not therefore possible to 'reclaim' the full amount of traffic received by the website). Examples of these types of action might include the deactivation of an e-commerce website offering the sale of non-legitimate (potentially counterfeit) branded goods, or the removal from a parking page of pay-per-click links that may be directing potential customers to competitor sites. In these cases, it will generally be possible for the brand owner to reclaim only a portion of the misdirected traffic, so the ROI calculation must incorporate assumptions about what this proportion should be. For an e-commerce site selling only products relating to the brand in question (a 'mono-brand' site), or for a pay-per-click site featuring a close misspelling of the domain name of the official site (or some other domain name that a typical internet user might guess to be the official site for the brand in question), it might be appropriate to make the case that a greater proportion of the traffic received by that site should be intended for the brand in question and could therefore potentially be reclaimed following an enforcement action.

E-commerce marketplace enforcement

E-commerce marketplace enforcement (ie, the removal from marketplace websites of offers of sale of infringing items) is one area where it is possible to carry out two distinct types of ROI assessment: one can be carried out in advance of the roll out of a brand-protection programme (*a priori* analysis) and another following the completion of a series of enforcement actions.

Advance or *a priori* ROI calculation

An advance ROI calculation aims to quantify the potential ROI resulting from a programme of monitoring and enforcement that has not yet launched. This type of calculation can help a brand owner to build a case within their business for releasing the funds necessary to

TABLE 2: Basic components used in the calculation of potential ROI associated with the recovery of an infringing domain (input data shown in **bold**; assumed values shown in *italics*)

Inputs		Outputs
Daily number of visitors to domain to be recovered (based on web-traffic estimates)	→	
Proportion of repeat visitors (aggregated over a year)	→	Total unique visitors to site per year
		↓
Business conversion rate	→	
Average customer value/spend	→	Total recoverable revenue per year

> **E-commerce marketplace enforcement is one area where it is possible to carry out two distinct types of ROI assessment**

support the programme, as well as gaining an understanding of the required scope and scale of the service.

In the case of e-commerce marketplaces, this calculation is based on an initial 'sweep' across as many marketplaces as may be relevant to determine the number of results returned in response to a search on each site for listings relating to the brand in question. Following any necessary cleansing of the data – such as modification of the raw numbers to account for the fact that some of the returned results may be false positives (eg, listings referring to the brand name in some other unrelated context) – the calculation aims to determine the total number of infringing (and enforceable) items that are likely to exist on each site. This can be achieved by making (order-of-magnitude) assumptions, for every marketplace site, of the number of items featured in each listing and the proportion of listings that typically feature infringing (eg, counterfeit) products, usually based on prior experiences of monitoring and enforcing on the sites (based on this information, the ROI calculation can be carried out as shown in Table 3). The calculation is based on the principle that a certain proportion of customers (for which an assumed conversion rate can be used) who would have purchased a counterfeit item will instead purchase a genuine item if the counterfeit is made unavailable (via a successful enforcement action). There is also a requirement to assume the average price of a genuine item – this may need to vary across the marketplaces, depending on the mix of product types being offered for sale on each site.

Post-enforcement ROI calculation

Once a programme of monitoring and enforcement has been established, it is possible to then carry out additional ROI calculations to determine factors such as the total numbers and value of (infringing) items removed via the enforcement (takedown) actions. These calculations can make use of real data from the live listings, such as the (actual) number of items available in each listing and the price of the items in each case. Many brand-protection service providers will make use of monitoring technology that automatically extracts this information from the listings at the point of detection. Beyond this, it may also be necessary to apply corrections to the data, such as the introduction of data caps. This may be required if, for example, a listing offers an extremely high quantity of items, perhaps intended to imply that the seller can manufacture on demand as many as may be required, but not providing a true representation of the inventory volume actually held. In such cases, it may be appropriate to replace the apparent quantity on offer with a more realistic, lower figure, so as to prevent the calculated value of items removed being artificially high.

A post-enforcement ROI calculation will also represent a truer reflection of the content on each marketplace that is genuinely actionable; as part of the brand-protection service, it will often be necessary to review the listings in detail on a case-by-case basis, to remove false positives and determine whether the items are actually infringing and eligible for takedown, which is dependent – at least in part – on the IP rights held by the brand owner.

Assumptions regarding conversion rates, among other things, can then be used to determine the proportion of the infringing revenue that may ultimately be reclaimable by the brand owner.

TABLE 3: Basic components used in the (*a priori*) calculation (for a given e-commerce marketplace) of potential ROI associated with the removal of infringing listings from the marketplace (input data shown in **bold**; assumed values shown in *italics*)

Inputs		Outputs
Number of listings (based on an initial sweep/search on the site)	→	
Typical percentage of listings that are counterfeit	→	
Typical number of items available per listing	→	Total number of counterfeit items
		↓
Average item price (genuine item)	→	
Customer conversion rate	→	Total recoverable revenue

Other types of ROI calculation

The basic ideas presented above can, in general, also be modified or expanded for use with enforcement actions against other types of infringing online content. The ROI associated with the deactivation of a standalone e-commerce site offering infringing products would ideally need to make use of information such as the volume of goods being sold through the site. In practice, it is rare that such data is available to third parties, although in some cases limited information may be available through open-source investigation techniques (eg, cross-referencing the sites against online trade or import/export databases). However, failing this, it might be possible to make use of web-traffic information for the site, as well as analysis of the mixture of brands and product types on offer.

For other content types, relevant data to be factored into an enforcement ROI calculation might include figures such as:

- for social media – the number of followers or 'likes' for infringing profiles or listings;
- for mobile apps – the number of downloads; and
- for piracy or file-sharing – the number of individuals involved in illegally sharing copyrighted content (eg, 'seeds' and 'leechers' for digital files over BitTorrent).

Comment

The central idea of ROI analysis is that it provides a means of quantifying the benefits associated with a brand-protection programme of monitoring (to identify infringing content) and enforcement (to remove this content). ROI calculations can be carried out both in advance of the implementation of a brand-

> **It is important not to lose sight of the fact that demonstrable ROI is only part of the story for a brand-protection programme**

protection service, as a way of justifying the spend on that service, and also subsequently to the takedown process, to quantify the value of items removed and determine how much of the pre-existing misdirected revenue can potentially be reclaimed by the brand owner. This type of calculation is key to demonstrating the worth of the service.

It is important, however, not to lose sight of the fact that demonstrable ROI is only part of the story for a brand-protection programme. For a brand owner, having an awareness of how their brand is being used and misused online – even when enforcement is not possible – can have other, less tangible benefits, allowing the brand owner to make informed decisions relating to their marketing and product-development strategies. In addition – and perhaps most importantly – an effective enforcement programme, combined with other factors such as customer education and the use of product verification tools, can help protect the consumer base from the damaging effects of exposure to non-legitimate products and content, which will have a positive effect on trust and, ultimately, on the intrinsic value of the brand. WTR

CSC
251 Little Falls Drive
Wilmington DE 19808
United States
Tel +1 302 636 5400
Fax +1 302 636 5454
Web www.cscdbs.com