Online brand protection: further down the rabbit hole we go

Author
Stephen Ward

Online brand enforcement sounds like a strong term, but what does it really mean? How do you know when you need an online brand enforcement programme and what do you focus on? Should you focus on anti-counterfeiting measures, copyright infringement, phony domains or diversion of trade? There is no simple answer. This article aims to provide an overview of various issues that arise when planning an online brand enforcement programme and its practical applications. We hear every day that we live in a global community and can connect in seconds with clients and business partners around the world. We can create a website in a village on a remote island and advertise our own or someone else's goods from that location. So what does this tell us in a world where counterfeiting and unauthorised sales of goods are estimated to constitute 5% of the world's gross domestic product – worth an estimated $135 billion? We are looking at a marketplace that touches every brand owner in some way. So where do you turn in a world that uses words such as 'phishing', 'pharming', 'cybersquatter' and 'infringer'? You should have a good compass and an idea of what is out there to assist you in protecting your brand online.

Global protection strategies

This section touches on specific forms of online brand protection and provides an overview of what works and how to implement the strategies that have proven successful. Online auction sites have evolved from what was the gold standard of eBay to other sites, such as Alibaba, Amazon, Ubid, Ebid and Overstock. There are also regional and geographic outlets (eg, Craig's List) and other sites that provide sales of products from specific countries and regions. It is important to think globally, as when logging into your computer and the Internet, you are regionalised to internet service provider (ISP) results and search results based on your location. If you have markets in Asia and your problem is in Asia, you may want to consider hiring a company that has access to regional monitoring or programmes that can secure a true picture of what is out there. Many providers in the larger space have good programmes and can source a great deal of data.

The next issue is the sheer volume of data and the need for an individual to review it all, and make recommendations on what to follow up and make test purchases. While many monitoring companies advertise that they can also undertake investigation services, it is recommended to utilise a monitoring service for monitoring and an investigations service for investigations. They both play a role in online brand protection, but neither seems to cover both spectrums seamlessly. After receiving a large data dump of potential infringements, the results of the search must be culled for authorised sales, vendors and identification of products that are authorised, counterfeit, diverted trade or grey-market goods. From here, the list of targets can be streamlined and then submitted to a local investigations company. Having one entity do the searching and then

conduct the investigation can be problematic, as no standalone entity can provide this service in a uniform manner on a global scale. The main goal is to find a company that has personnel on the ground or a physical presence in the geographic region in which you are seeking to conduct the investigation. Local or regional agents can assist the programme through their ability to understand the local language and culture. A regional address will also assist in quicker procurement of samples and the ability for the monitoring service to make offline contact with potential infringers. Buying counterfeit goods that are advertised on a local auction site in China from the United States can create issues that delay the procurement of the infringing samples. Once the search results have been reviewed, the scope of the investigation should focus on sellers that are selling multiples of the brand owner's products. These are identified as high-value targets. The initial purchase establishes a connection; the second purchase establishes trust; and the third purchase allows the investigator to gauge whether the seller has a constant pipeline and/or whether it has back flow or goods that were diverted. This may also smoke out a high-value target and convince it to meet with the local agent in order to secure more data relating to its supplier and source. In some cases, one seller can be the key to identifying a large-scale diversion of products or counterfeiters.

Continuing to police the market

Once the brand protection programme is online, data will be coming in from your search and monitoring company. You will have assigned your buy list to your investigators or be doing this yourself. What is the next step? After an initial six months, the market should slow down, unless a new product launch is underway. A common mistake that brand owners make is reducing the amount of online brand protection. There is one constant when it comes to e-commerce and the Internet: the market continues to expand and grow. As such, brand owners should not cut back after they see results in the online marketplace. It costs more time and money to seesaw when it comes to online brand protection than to maintain a steady programme.

The purchase of evidence by an internal employee is an accepted and practised method, but as the brand grows, so too does the need to expand the ability to police. There has been a recent trend of cases where internal employees are targeted in order to impeach their credibility and ability to testify to the methods that they used. There have been cases in which brand owners mistakenly shut down the website of a party which had right of first sale or was an authorised reseller. Some of these cases focused on the premise that the internal employees had no experience of online brand protection. However, in many cases we find that internal employees know the brand well and know what to look for. Internal employees have a good handle on the online market and an effective methodology which they follow. However, caution must be exercised, for practicality comes into effect when you are no longer making 80 purchases a year, but 80 per month or week. Brand owners must have strong internal programmes in place that use online forensic programmes enabling the purchaser of a sample product to take a forensic snapshot of the website that is selling and advertising the product. Such a programme will eliminate any doubt that the goods in question were secured from the suspect website. The forensic snapshot has a digital evidence hashtag and allows the advertisement to be preserved and used in court. Programmes such as this also enable a target's Facebook page, website and online footprint to be tracked, monitored and captured for preservation and future review. As a brand grows and matures, the brand owner must invest further in online brand protection.

Tools of the trade

Several tools are available that enable online brand protection specialists to conduct a reverse WHOIS search of an online infringer to source all active websites that are listed to it. Reverse WHOIS searches are effective only for infringers which register their websites to a name and address or email. The search provides a list of the websites that are registered to the target infringer. In some cases, a list of websites that are listed to one ISP block can be obtained; this allows you to try to target all of the infringer's websites in one go, as opposed to a 'whack-a-mole'-type approach.

Another valuable resource is the use of import and export records. In the United States, these services can track the number of shipments that an infringer receives. The service works in a similar way to a reverse WHOIS search, as it relies on contact data and information secured from your online monitoring service. Once you have this data, you can track down the number of shipments to a location, the exporter's identity and the country of origin. These services have also been effective in tracking importers and resellers of counterfeit goods. In a recent case, we found several high-value targets selling a popular product online. We backtracked the high-value targets' names and addresses through an import and export programme. We discovered that they all seemed to have one Chinese company in common. From this information, we were subsequently able to backtrack to all targets to which they had sold. This data allowed us to identify online sellers that we were not yet aware of before they became a problem, thus allowing us to stay ahead of the curve.

The use of online auction monitoring services is effective; however, there are limitations when dealing with sellers which use Amazon. In many cases, goods coming from Amazon are shipped from a fulfilment centre, not from the infringer. Using a test buy to secure the potential infringer's identity does not have a high ratio of success. Unlike eBay, Amazon in many cases owns the goods, so it may be contacted or even thought of as a potential third-party infringer.

It is imperative for your programme to have multiple strong cover identities so that the targets that you monitor do not catch on and expose you. The use of international voicemail providers allows you to have a regional exchange and to monitor calls. The use of post office boxes in regions throughout the world is necessary when dealing with infringers which do not ship globally. Brand owners should have several fully interactive websites with email. You cannot make multiple purchases without having multiple cover identities. However, the most important aspect of undertaking any type of *sub rosa* investigation with the use of cover identities is to follow the rules of law and not create situations where the data and evidence collected cannot be used in a court of law.

The tricksters are at it again

When protecting multiple brands online, a brand owner can identify certain trends in online infringement on the market. Many infringers register domains that are similar to the brand owner's; in some cases, they register the actual domain with the brand owner's name in the URL. We have found that the use of YouTube as a forum for selling infringing goods is becoming more prevalent, as is the act of contacting sellers and buyers in video game chatrooms. As the tools of the trade improve, the adversary adapts and overcomes. While in many recent cases we have seen a great number of brand owners resort to the mass shutdown of websites in one fell swoop, this does not stop the infringer; rather, it scatters the infringer to non-formal outlets and the problem remains unsolved. Infringers continually adapt. For example, a trend in Eastern Europe is to use phony websites and mobile phones. Infringers act as shipping companies and pick up real loads destined for locations in Europe and abscond with the goods. Then, shortly after the crime, the goods appear for sale online. In some cases, the infringer contacts the brand owner and tries to sell the stolen goods back to it, or it sells the goods to the brand owner's outlets. Another recent trend is the application of counterfeit branding at sea, as opposed to in a factory. Thus, brand owners must be vigilant and monitor all forms of online trade in order to adapt to infringers' activities.

Embedded analysts – the way of the future

A newer form of brand protection is the use of embedded investigators who focus solely on online brand protection programmes. This tool has been used by large enterprises with a global footprint which are concerned that a small team operating from one location is insufficient to combat the rise of online infringements. These so-called brand protection agents are normally engaged by a third party that employs and trains them. The main goal of brand protection agents is to focus on brand protection in an online form. Agents are trained to use best-of-breed solutions; in some cases, these include services that are not

offered by their employer, but which are most appropriate for the client. They manage local and regional assets, and are familiar with the field and associated costs. Many of the larger automotive programmes have turned to this type of service. An embedded brand protection analyst has local language skills and is familiar with local culture. He or she is dedicated solely to online brand protection and does not split his or her time on multiple tasks unrelated to brand protection. He or she is fully trained and up to speed on all modern investigative techniques. In many cases, brand protection agents augment search service results by conducting their own searches and scans using the client's technology. An embedded analyst can benchmark the growth of infringers in a region and provide real-time assessment of the client's ability to undertake enforcement within the region. In some regions of China and Turkey, the likelihood of a successful raid or enforcement action may hinge on the involvement of someone with knowledge of the culture and the limitations of the legal and criminal systems. Using this type of analyst allows the client to engage a dedicated person solely for the purpose of online brand enforcement. In many situations, the online brand enforcement role is assumed by a person who splits his or her focus on multiple tasks. The ability to make test purchases without having to outsource the service is an added benefit. As brand protection agents are specially trained in brand protection, they can be called as witnesses regarding investigations; this eliminates the concern of having an employee act as a witness in multiple cases.

Conclusion

No brand can afford to ignore the need for online brand protection. While global connectivity is growing by leaps and bounds, it is only natural that infringers will use the online market to abuse and make a profit from brand owners' names and products. The use of regionalised assets and a portfolio of multiple tools is the best course of action that a brand owner can take to address threats and meet them head-on. The more that a brand owner takes a strong, proactive approach to protection and policing, the more likely infringers are to shy away from its brand. It is said that imitation is the sincerest form of flattery, but not at the cost of one's reputation and goodwill. The negative impact that counterfeit or sub-standard goods entering the marketplace can have on a brand is not something that you can put a value on. WTR

Pinkerton
61 Broadway, 18th Floor
New York NY 10006, United States
Tel +1 212 480 0480
Web www.pinkerton.com

Stephen Ward
Vice president, East Coast region
stephen.ward@pinkerton.com

Stephen Ward joined Pinkerton in 2011 as a managing director and is currently vice president in charge of East Coast operations. He has more than 20 years of investigative experience as a lead investigator in more than 16,000 cases involving issues that range from computer data manipulation to complex money laundering and counterfeit interdiction.

Mr Ward manages all aspects of operations and investigations for clients seeking investigation services related to IP rights enforcements. He undertakes detailed investigations in the areas of copyright infringement, patent infringements, theft of trade secrets and white collar crime stemming from the redirection and/or misuse of intellectual property.