Online Brand Enforcement 2014

Protecting Your Trademarks in the Electronic Environment

Corporation Service Company

Safeguarding brands in the fast-changing digital space

Authors
Gretchen Olive and **Mark S Calandra**

Protecting intellectual property has always been a complex undertaking. In the pre-digital era, brand owners at least had a measure of direct control over their brands. Today, the rapid evolution of digital media is making it harder than ever to protect trademarks online. It is remarkably easy (and cheap) for anyone to hijack a brand and siphon off its value, whether by creating a bogus website or by starting up an unauthorised social media account.

So how can you protect your brand when it appears in so many different digital spaces? This article considers the challenges that trademark owners face in each area and examines strategies for overcoming them.

Your digital footprint is growing

The problem is that your brand's digital footprint – how online users perceive your brand online – is most likely bigger than you think and growing all the time. In addition to geographic or country web domains and email addresses, it includes social media handles and pages, mobile apps and blogs. A growing number of companies also have a 'shadow' digital footprint, with unofficial expressions of their brands, which is capable of diverting traffic, spreading misinformation, stealing data and distributing malware. The first step in safeguarding your brand online is to take a look at the size and shape of your digital footprint so that you can tailor a strategy to fit.

This article examines the brand protection issues that relate to each part of an organisation's digital footprint, including new generic top-level domains (gTLDs), and subsequently proposes a strategy for safeguarding intellectual property online.

Direct visits

According to the Optify B2B Marketing Benchmark Report 2012, typing a website address into a browser drives 40% of business-to-business website traffic. That is nearly as much as organic search (arriving at a site via a popular search engine, such as Google). The arrival of more and more gTLDs in the coming months and years will boost direct visits.

The recent experience of a large online content-streaming provider illustrates the potential for fraud. A *doppelgänger* domain – similar to the brand owner's, but omitting the dot after 'www' – managed to receive 300,000 visitors annually and also to distribute malware. This is not an example of just stealing traffic; it involves brand damage.

Whether it is a case of cybersquatting or typosquatting, brand infringements such as this are costly and can have long-term consequences. The good news is that there are many defensive and enforcement options for trademark owners. Start with a close and critical review of your domain portfolio. Ensure that you register all domains with high traffic and infringement potential. Enforcing your brand and trademark rights by issuing cease-and-desist letters, filing Uniform Domain Name Dispute Resolution Policy (UDRP) actions and Digital Millennium Copyright Act notifications, and, in the case of the new gTLD

programme, registrations with the Trademark Clearinghouse, along with well-developed registration, blocking and monitoring strategies and utilisation of the Uniform Rapid Suspension (URS) system, may all be needed to combat online infringement.

Search

It is not just brand owners which are developing excellent search engine optimisation (SEO) skills. Fraudsters, too, use best-in-class SEO techniques to divert traffic away from legitimate websites and towards bogus sites in order, for example, to sell counterfeit goods. The above-mentioned e-commerce company which had problems with a *doppelgänger* domain also experienced unauthorised competition in paid search, with a lookalike URL receiving 96,000 visitors annually and diverting searchers from genuine, paid-for results.

The challenge in this case is to find out whether your marks are being used in keyword search terms and to understand which websites, apart from your own, are optimised for searches that contain your trademarks, thereby potentially diverting traffic from your site to bogus or imposter sites.

Mobile

As smartphone and tablet commerce continues to grow at a breakneck pace, so does the range of branded apps at popular app stores. While channels such as these offer new opportunities for brands, they also create new possibilities for brand damage or worse. Bogus apps cover the full spectrum of harm, from providing a poor user experience to making money from your hard-earned reputation, or even taking over a user's operating system and illegally acquiring valuable data. If mobile apps are part of your digital footprint, it is important to monitor app channels and ensure that apps which are abusing terms and conditions or your trademark rights are removed.

Email

Email is highly valuable in retail, where approximately 30% of repeat visits by online shoppers are prompted by an email from a familiar brand, according to the Optify B2B Marketing Benchmark Report 2012. For business partners and existing customers already receptive to your messages, it remains a powerful tool. However, phishing emails can rapidly damage trust in a brand. Phishing scams cost the global economy billions each year, with more than 1,000 new phishing sites appearing every day, according to the Anti-phishing Working Group (www.apwg.org). The variety of targeted industries is growing, as well as the number of affected brands, so you can see how this can be a major problem. It used to be that only the giant companies and financial institutions had a target on their backs; but as users become more wary of their personal information on sites that are common phishing targets, the phishers have had to adapt and target a wider array of verticals and companies. Regular monitoring of the email channel, the use of email authentication (a service that stymies imposters by verifying the email's sender) and the ability to shut down infringing accounts quickly are all effective ways to ensure the integrity of this important route to market.

Social media

There is no question that social media is being taken seriously today. When a popular media outlet's social media account was hacked in April 2013, a fake message about explosions in the White House briefly knocked $135 billion off the value of the Standard & Poor's 500. Not only can social media handles and pages serve as an extension of a brand online, they also influence the responsiveness of search engines. As a consequence, fraudulent social media activity can cost brands traffic and damage their reputations. The above-mentioned e-commerce company was also plagued by bogus social accounts that used credible names to attract followers. A fake social media account set up in the company's name garnered more than 3,000 likes, and its unofficial social media presence had nearly 6,500 potentially valuable followers.

New gTLDs: your digital footprint is about to get even bigger

No one concerned with protecting trademarks in the digital space can ignore the arrival of the new gTLDs. While today there are just over 250 top-level domain extensions (eg, '.com', 'co.uk', '.org' and '.info'), over the next few years it is likely that there will be more than

Figure 1: **Managing your brand online: a three-part strategy**

	Key digital channels				
	Direct navigation	**Mobile**	**Search***	**Email**	**Social media**
PROTECT		URL Strategy (Brand Advisory) Domain name management SSL certificates DNS services			Social media username strategy Social username management
MONITOR	Domain name monitoring	Mobile app monitoring	Internet monitoring	Email monitoring (Phishing detection)	Social media monitoring
ENFORCE	Domain recovery (UDRP/DRP) Domain acquisitions	Mobile application removal	Search engine delisting Auction delisting	Website takedowns (Phishing & advance fee fraud) Domain recovery	Social media username takedown Social media content takedown

1,000 new extensions added. These will cover generic areas (eg, '.sports'), brand names (eg, '.canon'), geographical areas (eg, '.london') and communities (eg, '.eco').

For trademark owners, it is the hundreds of 'open' extensions that should be of immediate concern. For example, if you are a sports brand, you will need to decide to what extent, if any, you will want to use '.sports', weighing up both the opportunities and the risks of inaction. The Trademark Clearinghouse can help: a rights protection mechanism set up to support the new gTLDs, it is a single, global repository of verified trademarks. Its use is mandatory for anyone wanting to register domain names within a sunrise (pre-registration) period for any new gTLD. It will also notify brand owners when someone else tries to register a domain name that matches their trademark for a period of 90 days after each new gTLD is actually launched.

However, the Trademark Clearinghouse cannot solve all potential problems. While claims notices will help for a period of time, the clearinghouse provides no type of domain blocking services, so it is really up to the brand owner to know what is being registered and to register domain names defensively that are of importance to its brand(s). Other rights protection mechanisms have been introduced by some of the new gTLD registry operators, and are intended to be an extension of the Trademark Clearinghouse. However, these vary among the registry operators and involve different fees, so it is important to know what is out there to protect your brand in the new gTLDs and take necessary action accordingly.

According to Gretchen Olive, director of policy and industry affairs at CSC Digital Brand Services: "Companies have their hands full with '.com', '.net' and the various ccTLDs already today. The new gTLD programme, while posing a wealth of great new opportunities for businesses around the globe, has the chance to pose additional risk to brand owners as well if a strategy is not in place to make sure their trademarks, brands and other forms of IP are properly protected."

CSC recommends several steps for any organisation looking to protect its brands in the new gTLDs:
- Determine which trademarks to file with the Trademark Clearinghouse;
- Understand the other protection mechanisms available to you and adopt those that fit your strategy;
- Analyse and narrow the field of potential new gTLDs that will have the greatest impact on your business; and
- Identify branded strings and generic terms of interest to you in the new gTLDs.

In our experience, the best way to safeguard brands in the digital space is to adopt a strategy that covers your whole digital footprint, as shown in Figure 1 above. Putting in place the right protection measures minimises the chance of infringements in the first place, while a robust monitoring approach will help to ensure that you catch fraudulent activity before it can do significant damage. And when it becomes necessary to have recourse to enforcement, knowing the right steps to take gives you the best chance of shutting down infringement quickly and effectively.

Protection

Good protection strategies reduce the need for more time-consuming and costly enforcement action. However, for your trademarks to be adequately protected online, it is important to take a holistic view. This means looking at the full extent of your digital footprint – from established properties, such as geographic domain names and email addresses, through to social media usernames and the rapidly evolving ecosystem for mobile apps.

Acting early is important when it comes to protection. Registering domain names and social media usernames in advance of when they are needed helps to ensure that you own the relevant brand 'space' and shut out fraudsters. This is particularly important in social media, where – without a governing body to oversee the allocation of names – recovery and enforcement can be messy and time consuming.

For email, authentication is a key area to address. Ensuring that messages come from an authentic source and not an imposter filters out phony senders and reduces the risk of customers receiving brand-damaging communications. And for all channels, all of your digital intellectual property should be centrally managed, so that you can identify and deal with potential issues as efficiently as possible.

Monitoring

Monitoring is an important aspect of your online brand protection strategy, as it will allow you to understand what types of infringement are occurring in relation to your brand. However, an effective monitoring strategy is not just about identification. How do you prioritise which infringements to take action

on and which to let go? A domain name selling counterfeit goods or diverting traffic from your authentic site would be a higher priority than a social media page with a few followers with negative sentiment posted. It is important to understand what is out there, but also ensure that you are fighting the right battles that hold the most potential for brand erosion.

With the constant change in the numbers and types of key digital channel, it is critical to consider the numbers here. Formulate a strategy that identifies the actionable infringements that people are seeing and which run the risk of negatively affecting your brand. It is not possible to take action on everything, let alone find everything that is out there, but a proper monitoring and enforcement strategy will go a long way in ensuring that your brand stays as intact as possible.

Enforcement

The unfortunate truth is that sooner or later, many brands will need to take enforcement action. The good news is that there is a toolkit of options available.

For domain name issues, the UDRP requires that most types of domain-name dispute be resolved by agreement, court action or arbitration before a registrar will cancel, suspend or transfer a domain name. The UDRP has recently been complemented by the URS system, which was introduced by the Internet Corporation for Assigned Names and Numbers (ICANN) specifically to address disputes within new gTLDs (see Figure 2). According to ICANN, the URS system offers "rapid relief to trademark holders for the most clear-cut cases of infringement". There is also the classic cease-and-desist letter, which, while potentially effective, can also be easily ignored.

Trademark owners in Europe are in a better enforcement position, because ignoring an accusation of infringement is not permitted, and the process to proceed with a dispute requires a much higher level of evidence of the infringing action in order to move ahead. Complainants can also be counter-sued for false accusations, helping to ensure that only legitimate cases, backed by solid evidence, are presented.

It is important for brand owners to leverage the available enforcement options across all key digital channels, including direct

Figure 2: **Three-phase brand monitoring process**
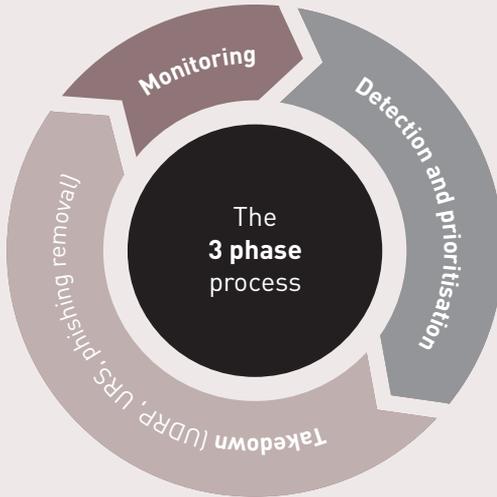
This chart illustrates the three-phase process of an effective brand monitoring strategy from start to finish. It is insufficient just to know what is out there; brand owners must also prioritise and take effective action against infringing parties.

will ensure that your efforts and budget are targeted appropriately.

Finally, trademark owners must be prepared to commit money and time to this area, especially when considering the increase in complexity presented by the addition of the new gTLD programme. For many brands, the upfront cost of defensive action will likely prove favourable compared to the potential costs and risk of infringement. **WTR**

navigation, mobile, email, search and social media. Each channel has its own unique threats and respective solutions to help mitigate infringement and enforce your brand rights.

Conclusion
No matter how far your brands extend into the digital space, with a systematic approach, it is possible to safeguard them online. The key is to understand the size of your digital footprint, so that you can be sure that the strategies that you adopt cover all expressions of your brand – from domain names to mobile apps.

An ounce of prevention is worth a pound of cure; thus, if you can proactively prevent infringement from occurring in the first place, you will be saving time and resources that can be put to other uses. Putting in place a comprehensive, end-to-end strategy for protecting and monitoring brands online offers far better value for money than constant legal and enforcement action.

That said, enforcement is sometimes needed, so understanding the options in depth

Corporation Service Company

DIGITAL BRAND SERVICES
CSC
CORPORATION SERVICE COMPANY

Corporation Service Company
2711 Centerville Road, Suite 400
Wilmington DE 19808, United States
Tel +1 302 636 5400
Fax +1 302 636 5400
Web www.cscglobal.com

Gretchen Olive
Director of policy and
industry affairs
Gretchen.olive@cscglobal.com

Gretchen M Olive is director
of policy and industry affairs
at CSC Digital Brand Services.
For more than 13 years she has
helped clients to navigate the
evolving internet landscape
through more effective global
domain name, trademark and
brand protection strategies.
Ms Olive is an internationally
recognised expert on the
Internet Corporation for
Assigned Names and Numbers'
(ICANN) new generic top-level
domain (gTLD) programme,
and to date has prepared nearly
100 new gTLD applications
on behalf of CSC clients. She
is an active member of the
International Trademark
Association (INTA) and the
Association of Corporate
Counsel, and since 2000
has represented CSC and the
views of its clients at ICANN
meetings around the world. She
has also served on numerous
committees related to INTA.

Mark S Calandra
Vice president
Mark.calandra@cscglobal.com

Mark Calandra has served as
vice president of sales and
product development for
CSC Digital Brand Services
since 2005. Before joining
CSC, Mr Calandra served
in senior management
capacities at two successful
start-up companies in the
corporate brand protection
space. His background also
includes marketing and brand
management experience at
Schering-Plough Corporation.
Mr Calandra holds a BA
in economics from Bucknell
University in Lewisburg, PA.
He received his MBA from
Columbia University in New
York, NY.