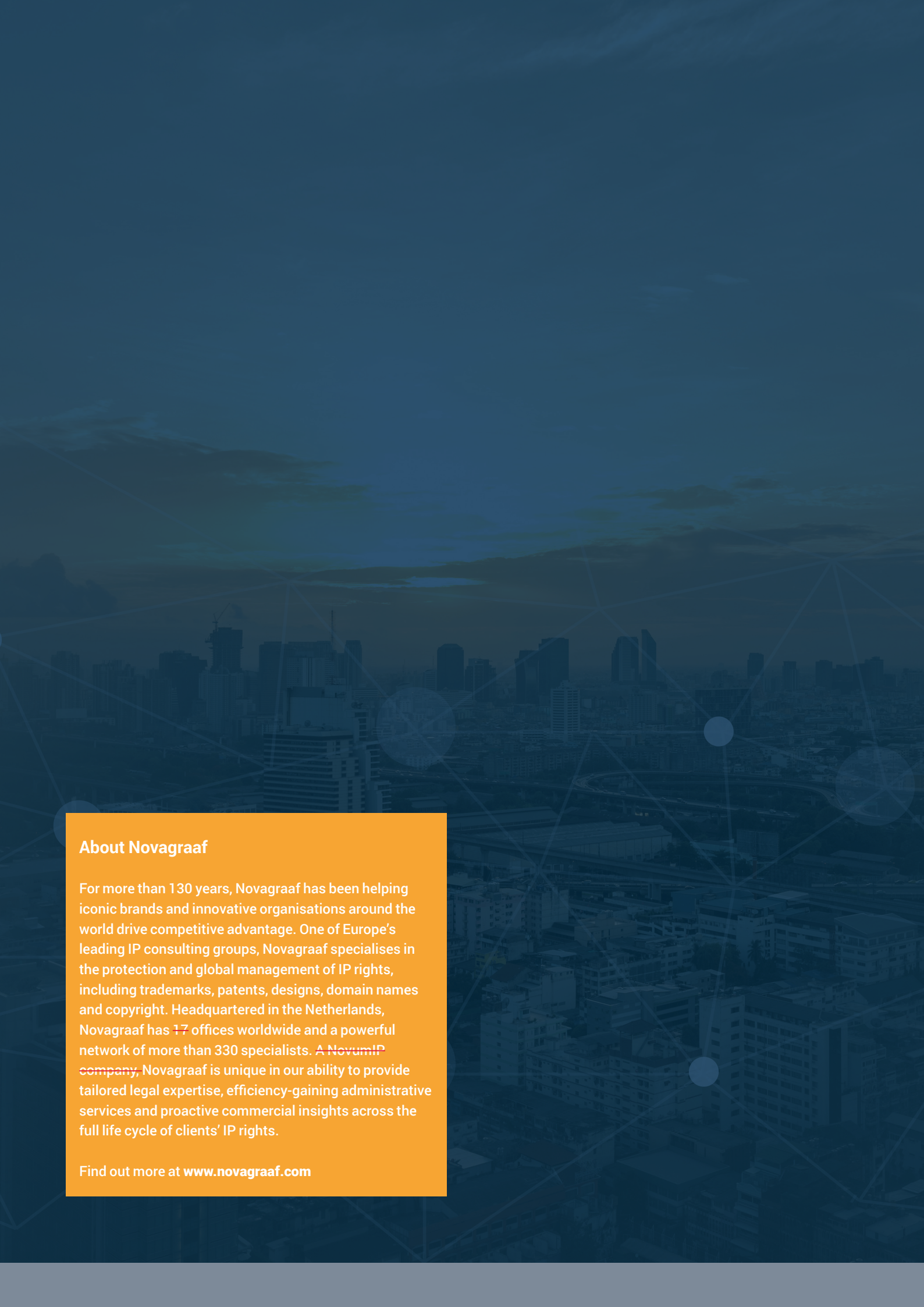
Novagraaf
A NovumIP Company

Novagraaf Expert Series: Online brand protection



About Novagraaf

For more than 130 years, Novagraaf has been helping iconic brands and innovative organisations around the world drive competitive advantage. One of Europe's leading IP consulting groups, Novagraaf specialises in the protection and global management of IP rights, including trademarks, patents, designs, domain names and copyright. Headquartered in the Netherlands, Novagraaf has ~~17~~ offices worldwide and a powerful network of more than 330 specialists. ~~A NovumIP company,~~ Novagraaf is unique in our ability to provide tailored legal expertise, efficiency-gaining administrative services and proactive commercial insights across the full life cycle of clients' IP rights.

Find out more at **www.novagraaf.com**

A brave new world for brand owners

The rise of technology has opened up new opportunities and new risks for brand owners, says Max Hübner.

The world was already feeling the impact of technological change when Aldous Huxley wrote his novel *Brave New World* (1931). It was released in an exciting new era of industrial speed and productivity, driven by key scientific advances and their application to mass production, as exemplified by Henry Ford's moving assembly line. This was also the start of new ways of working, with the artisan economy, based on craftsmanship, evolving into a new economy, based on modular systems of production.

Of course, not everyone was excited about the speed of change at the time. Huxley himself warned against its impact, setting out a frightening vision of the future in his novel and arguing that society and, more importantly, individual identity was at jeopardy due to the fast pace and uncontrollable effects of that transformation. In his eyes, these new technologies were not a sign that humankind had become more refined or civilised, but rather that it had been blinded by utopian ideas and the misleading opportunities offered by the first machine age.

Less than a hundred years have passed since he wrote his novel, but we can still recognise many of those concerns. In particular, the idea that machines and technology will threaten the livelihoods of workers is something that is still being discussed today, including in our industry: intellectual property (IP). In addition, we have new challenges and transformative events to negotiate, such as the impact of the COVID-19 pandemic *(see page 5)*. That seismic global event has thrown our traditional ways of working into sharp relief, impacting lives and livelihoods, and transforming us all into remote workers.

The question is now: will businesses try to spring back to old ways of working or will they be brave enough to readjust and embrace the possibilities of this new era?

Entering new horizons in professional services

Technology has already modernised the ways that businesses work of course, but the IP and legal sector has often been criticised as being slow to evolve and adapt. It's true that conventional wisdom has kept the 'artisan shop' of professional knowledge away from new ways of delivering services.

For a long time, it has held on to the traditional logic of bespoke services and hourly fees, and only really applied technology and automation in order to optimise its traditional ways of working (indeed, many firms still do).

However, as Richard Susskind predicted back in 2008 in *The End of Lawyers? Rethinking the nature of legal services*, IT and commoditisation have had a major impact on the provision of legal services in the 21st century. For most legal firms, technological transformation has now passed the tipping point. This is especially the case in the IP field, where more and more activities no longer belong to the exclusive domain of the legal professional. The industry has shifted from bespoke (tailored) through standardised (re-use), systematised (automated standardised) and packaged (on demand) to commoditised (non-value services), and this shift has led to the introduction of new business models for legal and other professional services.

This is a trend also set by us at Novagraaf, since we have worked over the years to apply the benefits of technology to our services, so as to add value and enable clients to manage their IP portfolios more efficiently and effectively. We did not want to settle for the status quo, but instead were brave enough to embrace the potential of technology and look to new horizons. Building upon our deep customer knowledge, first-rate service and rigorous attention to detail, this has included introducing new trendsetting solutions for our clients, thereby driving more value. We believe that this approach will become even more important as we adjust to the post-COVID-19 realities, including the predicted economic downturn.

New solutions for brand owners

We have focused on creating new solutions with and for our clients that combine our broad IP competence and process-oriented administrative services with new technologies and automated ways of working. Each combined service is designed to meet a client's need and tackle one of their market realities, helping them to work smarter and to achieve more with less. Our Online Brand Protection service, for example, has been designed to eradicate the pressure on resources (time and money) that is traditionally associated with monitoring and enforcing brands online.

Will businesses try to spring back to old ways of working or will they be brave enough to readjust and embrace the possibilities of this new era?

In a world in which complexity and continuous connectivity have become the new norm, the old approaches to online brand protection are no longer fit for purpose, so we challenged ourselves to find a better solution. The result is a fully integrated automating monitoring and enforcement tool that provides instant access to predefined results, enforcement workflows and tailored professional attorney advice via a single point of contact. We believe that this new tool and the strategies that we share in this white paper will help you to also prepare your brand and businesses for the current era and the challenges we face today.

Max Hübner
is Managing Director of Novagraaf Netherlands and a frequent speaker on the topic of legal operations and the future of IP legal services.

He can be contacted at brandprotection@novagraaf.com

You can find out more about our Online Brand Protection service by visiting our website at: www.novagraaf.com.

Setting a strategy for a post COVID-19 world

The COVID-19 pandemic has added extra pressure on (and opportunities for) brand owners, as consumers turn ever more to online channels for goods, services and information. Anca Draganescu-Pinawin sets out how to establish and execute effective online brand protection strategies that won't drain your valuable in-house time and resources.

Online retail has ramped up in recent years, giving more and more people access to goods and services, some previously unknown or unavailable to them, and adding a new level of convenience that conventional shopping cannot match. With the COVID-19 crisis further accelerating our use and reliance on online tools, has become normal to receive almost instant delivery without having to leave the house to shop.

In only a short span of time, we have seen an unprecedented and significant rise in online demand for goods, services and information, effectively supercharging the online environment. As people were driven out of the public square and into 'lockdown', they have turned to the online environment to meet their needs, whether for work, retail, news, exercise or communication.

The practical impacts of this for companies providing these products and services have been manifold. Many industries have seen an acute increase in demand for their goods but, in many cases, have also run into supply problems. Some have faced financial ruin, unable to cope with the move from the high street to online retailing, or competition with their more established e-commerce competitors. Still others have thrived, as consumers turn to new suppliers for recreational goods and services to stave off boredom at home, such as books, games, streaming services, and alternative forms of work and social interaction.

Identify and assess the threats

The rise in online commerce provides a big opportunity for brand owners, but there are also a number of specific IP risks to consider in relation to COVID-19 and the online market in general. In particular:

- *Brand infringement: undermining trust in your brand name*

This affects everyone from global health organisations to local businesses. In fact, the World Health Organization (WHO) has called the hijacking and fraudulent use of its brand, and others like it, to share misinformation or profit commercially, an 'infodemic'. Since logos function as shorthand for factual accuracy and reliability, many people consume this information uncritically. Brand owners need to be proactive in monitoring and enforcing their IP rights online, if they are able to act effectively and proportionately against the threat.

- *Buyer beware! Price gouging and counterfeit goods*

The surge in demand for medical products, such as hand sanitiser, masks and protective gloves, in addition to established retailers' inability to supply these goods, has created ideal conditions for third-party vendors to fill the gap. This, in turn, has led to price gouging as third parties have sought to profit from the panic. While many of the most egregious examples were quickly shut down by the online marketplaces, it is still possible to find such products online at a higher than normal price due to the spike in demand.

During the pandemic, there have also been many reported instances of faulty equipment, expired products, outright fakes and purported miracle cures, including expired face masks, hand sanitiser, counterfeit treatment kits, at-home testing kits, and coronavirus vaccine kits. Counterfeit goods have been a problem since the first days of e-commerce, but now with a chaotic market of buyers rushing to snap up available products as quickly as possible and sellers seeking to profit from increased demand, this is even more the case.

A further problem that emerges with third-party vendors is that of product quality. Buying products online involves a certain leap of faith. After all, you cannot verify the quality of a product nor the reliability of your vendor, as you might in a shopping centre, at the supermarket or in the retail district of any city. The moment of truth comes when the package arrives in the mail.

- *Domain name profiteering, phishing and malware*

The key issue in the case of both information and product quality is that of trustworthiness. Naturally, we trust those brand names that we recognise, that have cachet and authority, or that are shared with us by trusted sources, including on social media and in the search rankings of search engines.

Given that domain names function like shop signs online, it's no surprise that they are often the first target of fraudsters seeking to misdirect online traffic or otherwise profit from unsuspecting consumers. While there are well-established procedures in place to act against cybersquatters, it would be a mistake to think that brand owners are winning the battle to protect their brands from malicious domain name registrations. In fact, the harm caused by such registrations should be of as concern to brand owners as that of social media platforms and online marketplaces.

In addition to misinformation and the sale of counterfeits, domain names are also used for speculation, where domain names containing terms that have the potential to attract a lot of traffic are bought up with the prospect of selling them at a profit. For instance, domain names including terms such as coronavirus, covid, vaccine, diagnostic and testing. This has led some registrars, such as Namecheap, to tighten control over certain keywords and to remove words such as 'coronavirus,' 'covid,' and 'vaccine,' from search tools. On the ccTLD front, EURid and Nominet have, for their part, put in place procedures ensuring that the .eu and .uk namespaces are free as possible from domain names registered for exploitative or malicious purposes.

Even more dangerously, some domain names have been launched that mimic widely recognised authoritative or official sources (lookalike sites) to signal trustworthiness and reliability with regard to information. Official agencies have acknowledged the high risk of their names being appropriated for phishing and other forms of cyberattack. The sudden rise of online communication tools to respond to social isolation imperatives has in turn inspired a rash of phishing websites that seek to direct traffic to themselves by mimicking major brands and legitimate platforms *(for more on this topic, see page 9)*.

Routes to protection

The need to maintain brand reputation, protect your business and customers from exploitation and counterfeiters, and to shore up your digital presence against domain name squatters should already have been high on your IP strategy for 2020. However, the COVID-19 outbreak will have heightened that focus – and for good reason.

To maintain trust in your brand requires an act of foresight to develop an online brand protection strategy that will both protect your brand and provide it with the conditions to flourish in the online world, both today and tomorrow. This will ensure that when your customers reach out to you online they can rest easy knowing that it really is you that they'll find on the other side.

Anca Draganescu-Pinawin
is IP Counsel at Novagraaf in Switzerland and Head of Online Brand Protection at Novagraaf. Contact her at: brandprotection@novagraaf.com.

Back to basics: Getting started

A step-by-step guide for brand owners yet to establish an online brand protection strategy or those looking to update their approach.

STEP 1 Set your strategy

To establish an effective and proportionate online brand protection strategy, you need to first take a step back to define the scope of your activities, to identify the biggest threats to your brand, to define enforcement routes and budgets, and to develop a plan of attack that is proportionate to the extent of the threat and the available routes of enforcement action.

Not sure how to assess your brand's general condition online? Sign up for a free online survey of the threat landscape for your brand by visiting novagraaf.com/brand-protection.

STEP 2 Define your channels

Brand owners are at risk from more than that old foe: counterfeiting. The ways in which we all shop and communicate have opened up a range of new online channels that need to be monitored and policed. From a brand reputation and trademark enforcement perspective, we recommend focusing in particular on: apps, domain names, marketplaces, social media and web content. A joined-up strategy and common tool is recommended here (see page 7).

STEP 3 Make sure IP protection is in place!

Ensure you have registrations in place for all aspects of your product that could be at threat online, and in all markets/geographies of trade. This may seem obvious, but it is an area that is often overlooked. Without the appropriate registrations in place, enforcement procedures such as marketplace takedowns or domain name dispute resolution policies, may not be available to you, forcing you to take more expensive or remedial action to counter these common threats.

STEP 4 Automate where possible

Such is the size of the online market, it won't be cost effective (or even possible) to take action against every instance of brand damage. Focus instead on the biggest and most damaging threats, and target enforcement action and budget accordingly. Defining a policy that defines action and selection criteria will help here (see step 1), but so too will the use of a tool/service that automates common enforcement activities, such as takedown notices or cease-and-desist letters. This will also lower the cost of such activities, and help you to take prompt action.

STEP 5 Measure ROI

IP professionals know the importance of online monitoring and enforcement, but they also need to justify its cost. This can be hard when you're using a multitude of different systems and suppliers, or not using a common dashboard to track your activities and their impact. Fortunately, modern case management systems enable users to run quick and accurate reports, and provide the data needed to drive intelligent decision-making. If you don't have a clear picture of your activities, get in touch with us to find out how we can help.

STEP 6 Review your approach – regularly

The online market moves quickly, and so should you. That necessitates regular tracking and reviews to make sure you're covering all bases. Your strategy should also be updated when you enter new markets or geographies, or launch new products and services. Depending on your business and its risk profile online, we recommend regular reviews every 3-6 months to make sure your current policies are fit for purpose.

For additional insight and advice, please speak to your Novagraaf attorney or contact the team at brandprotection@novagraaf.com.

Focus on these five channels

In our experience, the following five content channels are the most important areas for monitoring and enforcement:

- **Apps:** While apps can help brands to increase and improve interactions with their consumer bases, and gather market intelligence, it is another area of potential brand abuse. Monitor for any apps and app publishers that mention a brand in the app name or as part of the publisher's name, providing brands with the insight they need to evaluate and take action.
- **Domain names:** Cybersquatting is a continuous issue for brand owners (see page 8). The most efficient approach here is to choose a domain name monitoring service that automatically identifies unauthorised use of a brand name in newly registered domain names, and proposes or automates appropriate courses of action, from simple surveillance of the potential threat to takedown actions and UDRPs.
- **Marketplaces:** It's important to monitor for potential infringements on major e-commerce platforms, such as eBay, Amazon, Alibaba, AliExpress, Tmall.com, Taobao and IndiaMART. Screening will provide valuable insights on how branded goods and services are being sold in the ecommerce market and provide the tools to remove those threats.
- **Social media:** Unfortunately, social media is an increasingly popular channel for counterfeiting and other forms of infringement. All major social media platforms should be monitored, including Facebook, Instagram, Twitter, LinkedIn, YouTube, WeChat (China), Weibo (China) and VKontakte (Russia), also identifying patterns and repeat offenders by checking account name and public feed.
- **Web content:** Look out for potential infringements in the online content of websites indexed by major search engines, whether or not the brand appears in the domain name, e.g. lookalike sites. This includes identifying threats to a brand on websites appearing in major search engine results, in links, page content, images (using image recognition technologies) and metatags.

Depending on your business, some or potentially all of these channels will require monitoring, and the more synchronised your monitoring and enforcement activities, the more effective and efficient they are likely to be. Find out how modern tools can help in this respect by signing up for a demo of our Online Brand Protection service at: novagraaf.com/brand-protection.

Additional resources

For more advice on protecting your brand assets, you can find the following resources on our website:

- *White paper*: Strategies for anti-counterfeiting: A practical guide
- *Microsite*: Online Brand Protection
- *Perspectives*: Subscribe to our bi-weekly IP newsletter for the latest news and advice.

Our IP attorneys are, of course, always available to answer any queries you may have. Get in touch at: brandprotection@novagraaf.com.

Screen your brand online for free!

White paper readers are invited to sign up to receive a complimentary online screening of one of their brand names. The analysis will identify threats to that brand online and propose ways to take effective and proportionate remedial action.

Find out more at **novagraaf.com/brand-protection**

Domain name focus

Cybercriminals and counterfeiters are finding ever more original and innovative ways of taking advantage of brand owners' rights, as Colombe Dougnac explains.

The types and extent of online infringement has multiplied in recent years and this trend only looks set to continue as e-commerce continues to grow. From a domain name perspective, cybersquatting, phishing, spam, copycat and counterfeiting are among the many infringements that companies and individuals have to face.

New threats to consumers and businesses have also emerged during the COVID-19 crisis, such as the wave of purchases of domain names featuring virus-related keywords, such as 'covid', 'covid-19' and 'coronavirus', and then 'chloroquine', 'deconfinement', 'test' and 'masks'. At one point, more than 6,000 COVID-19-related domain name registrations were being recorded per day, each potentially contentious or with the intention of malicious exploitation.

These domain names are then used either for resale (resellers wishing to take advantage of the crisis by auctioning domain names at prices of up to several thousand euros), or for sites calling for donations to fictitious associations, or to sell a counterfeit product, or for sites selling online products unrelated to the virus.

Infringing trademark rights

'COVID' is not a trademark of course, and more critical situations arise where third parties attempt to register a domain name using another company's trademark/s. For example, following an administrative complaint, WIPO's Arbitration and Mediation Center ordered the transfer of the domain name 'coronagileadsciences.com' to the rights holder, Gilead Sciences, Inc. (Litigation No. D202020-0776) on 5 May 2020.

Likewise, several registries in charge of registering country-code top-level domain names (ccTLDs) have taken measures to react against this exceptional wave of infringements.

The registry responsible for the management of .eu (EURID) has set up an Abuse Prevention and Early Warning System (APEWS), which makes it possible to detect potential abuse of a .eu domain name. In this case, the system delays its delegation in the .eu zone and puts the registration under a specific status of 'server hold', until the complete verification of this reservation by EURID. The British registry Nominet has also set up a system for suspending several hundred potentially fraudulent domain names.

Rather than relying on the registries to try to stop infringements, and since they cannot stop all infringements, right holders are also advised to take measures in order to:

- set up safeguards to limit the risk of infringement;
- detect and assess threats and/or infringements on all web media: apps, social networks, marketplaces, websites and domain names; and
- react quickly against fraudulent use of the trademark and strategically stop infringement.

Auditing the risk to domain names

Here, it is advised to begin with an audit of your existing domain name portfolio in order to identify:

- strategic domain names: website, e-commerce website, messaging, sub-domain, VPN…;
- defensive domain names which are less interesting but which could be prejudicial in case of registration by a third party;
- peripheral domain names that are of no interest (recovery following a complaint, old marketing campaign…) and which could be allowed to lapse to make savings.

Activities can then be prioritised according to the importance of the domain names, namely:

- Implementing of technical measures to secure domain names and websites belonging to the rights holder: This limits the risks of attack or at least makes it more difficult for such attacks to lead to diversion of traffic. This is the so-called 'Registry Lock' system, which makes it possible to block hacking through the authentication system managed by the registry. The idea is not to implement these security systems on all domain names, but instead target the most strategic domain names.
- Investigate: A request to lift anonymity or a request to check WHOIS data in order to investigate and pursue the domain name holder, in the event of fraudulent reservation of domain names under cover of anonymity.

- The establishment of a response strategy based on the damage caused: The choice and manner of response must be proportionate to the damage suffered or the risk of future damage. Indeed, several responses are likely to be sent to different recipients depending on the responsibility of each (provider, registrar, host...).
- Social media takedowns: Sites such as Facebook, Twitter and Instagram have online complaint procedures and are often considered as hosting providers. This grants them a lighter responsibility but with the obligation to take the necessary measures to stop infringement, as soon as they are informed.
- Extra-judicial procedures: many administrative procedures for settling disputes are now open to right holders, and they have the advantage of being quick, economical and efficient (recovery or abandonment of the disputed account or domain name). Depending on the extension of the domain name in question, the prior right invoked and the context of the situation, different options are available: for example, the UDRP complaint for generic top level domain names (gTLDs) and country code Top Level Domains (ccTLDs) or the URS complaint for new extensions.

The choice of procedure is not insignificant, since it depends on the situation and requires legal advice to determine the best strategy according to the use of the domain name, prior rights, the requirements and the goal sought. In order to be able to detect these 'cybersquattings' in advance, it is of course also important to set up a surveillance of your trademark among the domain names in order to react quickly and efficiently.

This monitoring should not be limited to domain names, but should also cover all relevant communication channels: apps, social media, marketplaces, website content and domain names (see page 7). This allows brand owners to quickly detect unauthorised use of the sign, to analyse the damage and to act promptly in order to stop the infringement.

Colombe Dougnac
is a Trademark Attorney at Novagraaf in France. She can be contacted at: brandprotection@novagraaf.com.

Why cybersecurity and online brand protection should go hand in hand

A more than significant increase in computer attacks has been reported since the start of the COVID-19 crisis. From fake websites to phishing campaigns and hacking, brands are being used and abused to help spread a different kind of virus. What can and should brand owners do? Yohann Conti from Pélissier & Partners offers some advice.

There are many teleworking, remote meetings and online file exchanges have always raised issues of data security, but the current health crisis has exposed ever greater numbers of businesses. Companies need to realise that their data is their treasure and that protecting it needs to be the number one priority in an increasingly digital world.

Start by changing mindsets

Protecting a company's information assets is not only the job of the IT department, but should be a priority for all employees, from the board of directors to the most junior recruit.

Why is this protection necessary? Because every employee has access to that precious corporate treasure: the company's information assets. That raises the possibility of both intentional employee theft and unintentional damage by an employee targeted by a phishing attack, as well as brand spoofing that can impact consumers as well as employees.

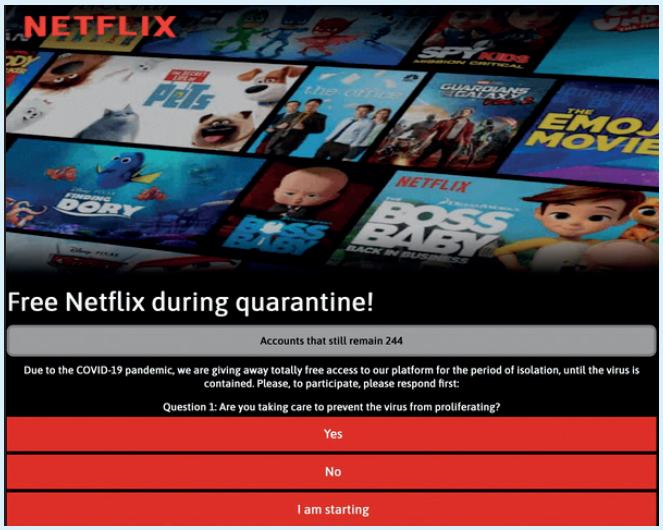
Netflix: Why nothing comes for free

Without doubt, the Netflix video-on-demand platform is one of the biggest winners of the global lockdown. Consumers might think that such a well-known brand with such a robust visual identity is fully protected, but IP professionals know differently. This message (see images p10) was received by tens of thousands of WhatsApp users in the US. The message, apparently sent by Netflix, promises a free subscription to help people endure the COVID-19 quarantine.

The link (https://Netflix-usa.net) looks like it might belong to the company, and when you click on it, it takes you to a page that looks as if it belongs to Netflix (see below). Surely, there's no reason to be suspicious?

Due to the CoronaVirus pandemic worldwide, Netflix is giving some free pass for their platform during the period of isolation. Run on the site cause it will end quick!

https://netflix-usa.net/?free-isolation-period



As with all things on the internet, it is always best to be wary, especially when the offer is so tempting.

There are some immediate giveaways: the typos, the requests for a certain amount of data that a company such as Netflix has no right to obtain and, of course, the demand that the link be shared with 10 other contacts before the account can be activated.

Those that overlook these warning signs for the promise of a free account do so at their peril. There is no free account on offer; instead, the Netflix brand is being used to trick people into providing confidential information and to spread the attack. The data collected will either be sold or used to carry out a much more targeted and dangerous spear phishing attack.

What can brands do to protect themselves?

This is a notable but sadly not unique example; although it does illustrate the ingenuity of hackers, on one hand, and the importance of domain name watching and defensive registrations, on the other. Clearly, a domain name as similar and potentially meaningful as Netflix-usa.net should not have been left available for malicious use.

Domain name watching and defensive registrations are key tools that enable brands to protect themselves effectively against cybersquatting and cyberscamming, i.e. the malicious use of domain names that are either legitimate or close to the original brand names. Allowing third parties to use such domain names opens the door to scam emails, phishing campaigns and other causes of consumer harm and reputational damage.

That's also why it's important to address cybersecurity issues as part of your online brand protection strategy. Taking the necessary steps to assure your working environment and data exchanges are completely secure is no longer an option in a world in which digitalisation is advancing at a rapid pace. A global security strategy led by experts in the field, as well as user awareness, needs to become the 'new normal' for businesses.

This means assessing data channels and risks in order to develop a cybersecurity strategy that reflects the company, its market and the ways in which its employees work. As important, that strategy then needs to be combined with its wider online brand protection activities, including domain name monitoring and enforcement. This is a must if you are to stop your brand playing a role in the spreading of computer viruses in a world already suffering from viral impact.

Yohann Conti
is Head of Cybersecurity at Pélissier & Partners (www.pelissier-partners.com).

Pélissier & Partners
Explorateurs de connaissances

Novagraaf
A NovumIP Company

Novagraaf's Online Brand Protection service

A modern solution to a modern problem

As specialist attorneys responsible for clients' IP strategy and implementation, we have the knowledge, background and global reach needed to integrate online brand protection seamlessly into the larger IP landscape of your business.

We understand the time and resource pressures on in-house IP and brand protection departments, and law firms. That's why we've developed an intelligent and fully web-enabled service that will inform you of relevant results, offer practical solutions in line with your wider IP strategy, and make effective strikes on threats to your online brand presence.

Our Online Brand Protection service captures the full risk picture online, facilitates enforcement actions and detects threat patterns to better track and take action against infringement:

- Enforcement actions are pre-defined, reducing the demands on your in-house teams;
- Common tasks are automated via a digital case management system (CMS), so that enforcement activities are rapid and cost-effective;
- Activity is targeted by type of threat;
- Monitoring and enforcement results are available via the online CMS, combining analyst and attorney expertise;
- The service is backed by Novagraaf's global network of IP attorneys, enabling additional enforcement activities to be taken rapidly and strategically, irrespective of geography.

The service includes an initial survey of the online threat landscape to generate a preliminary report of your brand's general online condition. This is used to determine the parameters of the monitoring and enforcement phases to best meet your goals and to pre-specify the necessary actions, the budget (per brand/module) and the triggers for any additional strategic activities.

Further information

Find out more at novagraaf.com/brand-protection or by contacting us at **brandprotection@novagraaf.com**.