

Protecting Domain Names in a Worldwide Context

Global Digital Encounters Encounter 16

Final Report

Date: October 14th, 2021

Speakers:

Malcom Bain, Partner at Across Legal.
Caroline Berube, Managing Partner of HJM Asia Law & Co LLC.

Moderator:

Joe Sekhon, Senior Lecturer in IP Law at the University of Portsmouth.

Introduction

Objective of the session: During, and further to the COVID-19 crisis, digital business, and access to digital information increased exponentially. The protection of Internet Domain Names became more and more important for business operators, and also for Organizations highly visible on the net, i.e., for society in general. The value of Domain Names thus increased exponentially, exposing them, and the IP assets they relate to, to cyberattacks, cyber-squatting and cyber-grabbing. How is /can IP Protection be currently further enhanced? What kind of consensus may exist in various parts of the world and in international fora for such an enhancement? For this Session of our Global Digital Encounters, Speakers from Europe, Asia, and North America with a variety of opinions will provide a worldwide picture of the future of IP protection connected to Domain Names, and for re-imagining IP in this area in favor of both business and consumers/society.

Preliminary remarks: Prof. Laurent Manderieux outlined that, with the COVID pandemic, and even further to it, the trend in business has moved from traditional operations to digital operations, where domain names have become more important. More than twenty years ago, mechanisms were put in place to further link the relation between domain names and trademarks and other IP rights in order to permit to fight against cyber-squatting, cyber-rubbing and other behaviors that could alter the trust in business: indeed, ICANN, the organization that runs the Internet system under "bottom-up" governance rules, promoted initiatives that led the World Intellectual Property Organization ("WIPO") and its member states, to develop administrative enforcement mechanisms for ensuring a smoother relation between domain names and trademarks. With the current pandemic, the digital age is further developing and therefore domain names have gained a new centrality in particular for their defense and protection.

Javier Fernandez-Lasquetty, pointed out that the matter of domain names created, many years ago, a first digital jurisdiction by the enactment of Uniform Domain-Name Dispute-Resolution Policy ("UDRP") rules and the administration of means for solution of conflicts such administrations such as WIPO.

Moderator, **Joe Sekhon**, laid the foundation by speaking about the need for discussion and conversation on domain names and the global challenges to this end. **The session took the form of Q&A (question and answer) session** with Joe Sekhon and the participants raising the below questions:

1. How an individual and/or organization could protect a domain name under current legal framework in the European Union?

Malcom Bain started the discussion exposing that, since the domain name is made of a name or a sign, the basic mechanism to protect or recover a domain name is trademark law. In this context, the easier way for domain name holders to ensure there is a legitimate right to be enforced against third parties is to have a trademark consisting of, or containing, the domain name. The latter, considering that UDRP system gives some priority to trademark holders.

In this sense, should the holder of a domain name have a related trademark, there are different alternatives:

- To launch a traditional court case claiming trademark infringement because courts may appreciate that the use of the domain name is a use in the course of trade.
- Using the arbitration UDRP process set up by the Internet Corporation for Assigned Names and Numbers ("ICANN") and WIPO or other centres.
- Should we refer to a country code Top Level Domain ("ccTLD"), some jurisdictions may have Administrative Bodies (Registries) with specific procedures to revoke and/or transfer domain names.
- In addition, if it is a competitor is using the domain name, also unfair competition could be claimed.

Finally, there is a pragmatic approach to protect from potential conflicts, which is to buy domain names. Preventive action, as opposed of protective action, is buying as many domain names around your brand as is reasonable in your context.

Joe Sekhon highlighted that buying related domain names is an advice oftentimes provided to start-ups. Moreover, he outlined that in the United Kingdom they do not apply, as

such, unfair competition, but the tort of passing-off, applicable where one company is using a similar domain name to another company and exploits its goodwill and reputation.

2. How an individual and/or organization could protect a domain name under current legal framework in China and Singapore? Can individuals register domain names in China?

Caroline Berube, pointed out that, ideally, companies would register a trademark and, afterwards, obtain a domain name. However, this is not always the case.

In China, in order to obtain a domain name “.com” or “.com.cn” a company has to go to the China Network and Information Center (“**CNNIC**”), managed by the Ministry of Information, that is part of the Chinese Government. Some characteristics are as follows:

- The main advantage of registering a domain name is that domain name registration is in both English and Chinese language while the trademark registration process is not completely in English. In addition, although the process for domain name registration may be relatively simple, companies must go to one of the sixty Registrars approved by the CNNIC.
- To register a domain name, companies also need to hold a “business license” in China, which is valid from one to five years for domain name registration. Companies without a separately registered Chinese subsidiary have been known to use the “business license” from another Chinese company, which may become a controversial issue because the domain name does not really belong to the company using the business license, but to the company that has provided the business license. In this sense, foreign companies wishing to obtain a domain name have to rely on “business licenses” from companies that they trust.
- A Chinese individual may register a domain name “cn”, but foreign individuals would have problems while registering “cn” domain names because the requirements are not the same.

In Singapore, the process is simpler since, for instance, there are no language barriers. A company should go to the Singapore Network Information Center and register the relevant “.com” or “.sg”. Companies may register through an agent and to the applicant will need to provide a local address, which is frequently that of the relevant agent. As mentioned about China, this may also become controversial if agent companies are not reliable.

3. One issue faced in the United Kingdom with cyber-squatting is that there are some individuals that may easily register the domain names for such purpose. Is this issue of cyber-squatting less prominent in China because there is a previous filter in terms of registration?

Caroline Berube, explained that, to some extent, this is right. However, it has to be considered that Chinese undertakings do not have the same limitations as foreign companies, therefore they may register as many domain names as they wish. As a result, there is still a lot of cyber-squatting.

With regards to available proceedings, one may go to the CNNIC to launch a dispute to claim that someone else registered a domain name in bad faith. Otherwise, a company can go to civil courts. In this context, there is a recent law that came into effect in 2020 regarding how the Supreme Court should interpret cases of cyber-squatting.

Malcom Bain highlighted that, whereas “.com” or “.net” domains may be easier to register, ccTLD are sometimes a little bit more restrictive. In Spain, for example, in the past a company had also to hold a trademark in order to be able to apply for a domain name. Now, albeit prior trademark registration criterion was removed, a company needs to have a link with Spain for the registration of a “.es” domain name, or the domain name may be challenged administratively.

4. A relevant question in this matter is to define what constitutes infringement. Could we expand on the concept of bad faith or malicious intent?

Malcom Bain observed that there are three conditions for claiming back a domain name back under the UDRP (summarizing): (i) having a legitimate right; (ii) the respondent not having a legitimate right; and (iii) the respondent having registered and used the domain name in bad faith.

Bad faith has to be proven both for registration and for use of the domain name, something which, sometimes is not very easy. The UDRP provides some examples of what bad faith is, which cover all behaviors that are negatively targeted towards prior rights of the claimant, such as monetizing the claimant brand, attracting internet users, away from the legitimate site, offering to sell the domain name back to the claimant, etc.

The concept of bad faith may suffer from some legal uncertainty, but does introduce some flexibility in the domain name system to enable respondents to defend themselves when, for instance, they are using a third parties’ registered trademarks in good faith or may have a good legitimate basis - e.g., when exercising freedom of speech.

Caroline Berube outlined that in Singapore bad faith would be the main factor for determining that the domain name was not lawfully registered, while in China the main criteria would

be the malicious intent.

The burden of proof is always on the plaintiff, and Chinese courts have proven to be very exigent with the plaintiff in proving the existence of malicious intent, meaning that taking an illegal profit by registering a domain name before another company has to be proven. In addition, she highlighted that damages granted in China are not very high, which adds an extra complexity for the plaintiff as he has to quantify its financial losses. In cases where there is a prior trademark being exploited by the defendant it may be easier, but there is a clear issue of whether the plaintiff is able to prove malicious intent on the part of the alleged infringer. In this context, there are relevant laws such as the Cybersecurity Law, Trademark Law and Unfair Competition Law that are relevant when it comes to cyber-squatting practices.

Malcom Bain stressed that in cases where there is a criminal activity such as selling of counterfeit goods or phishing it may be easier to prove bad faith and companies may not even need to prove such bad faith for a court to understand that there is a criminal offence. The strengthen of criminal and cybersecurity laws could help to address some domain name related issues, but this addresses only a portion of the market and cases of infringement.

5. Domain names have an online and international presence. Which are the main aspects of international domain name disputes? What the legal and jurisdictional obstacles are in terms of domain name disputes?

Malcom Bain outlined that, in terms of procedural aspects, identifying the registrant is difficult and it is getting more complicated with the use of privacy services to hide the identity of the registrant. Another aspect is that, albeit registrants may not be known, registries and registrars can be identified using tools as "whois". In any case, ICANN and the setting of a domain name system has diminished the opacity of the procedure.

Caroline Berube clarified that Singapore has not yet adopted the UDRP rules, which means that the claimant has to go to a Singapore court.

As to China, they are currently negotiating the adoption of the UDRP system, which entails that a company may either go to the CNNIC or to civil courts. On the other hand, in China, enforcement of a foreign judgment can be complex, therefore finding out where the defendant is located is paramount in ensuring the enforcement of any judgment.

6. Is there any impact of the vast amount of new Top Level Domain Names ("tLDN") that have been created in the past few years?

Malcom Bain observed that, albeit there are lots of newly introduced tLDN, a potential restriction is that some tLDN impose additional requirements for registration. For instance, in order to register a ".coop" companies may need

to be a cooperative registered in their respective jurisdiction.

The creation of such new domain names may entail that companies have to recalibrate their Intellectual Property strategy and the domain name strategy in light of their marketing strategy and evaluate whether it is worth acquiring such domain names, e.g, as a preventive action.

Related to this aspect, **Caroline Berube** outlined the convenience, from a marketing perspective, to evaluate which is the target of the company and whether such users normally use a ccTLD or a gTLD.

7. Considering consumption trends (e.g., shift from web sites to web apps), which will be the future impact on domain names? Is there any future roadmap with regards to domain name disputes?

Malcom Bain outlined that, in terms of e-commerce, apps stores could become a sort of "registrar" because they will be hosting an app with a specific brand. Therefore, we may be shifting from taking down a domain name to taking down a specific app. He also highlighted that disputes in the e-commerce space have to be better regulated, for instance: (i) there is a clear imbalance between the cost of purchasing a domain name, around 10 euros, and the legal fees to recover the same, around 3,000 euros, which could not act as a deterrent for potential infringers; and (ii) privacy law and the "WHOIS" problem, considering the increasing use of privacy services to mask the identity of the registrant which, at the end of the day, makes it difficult to identify the potential infringer - in this space, some previous screening regarding the identity of registrants could work to reduce the amount of potential infringers.

Caroline Berube agreed on the fact that there have to be more preventive measures to avoid domain name disputes such as the application of registration screening measures. She also made reference to the convenience of having homogeneous procedural laws regarding domain name disputes at an international level.

Malcom Bain mentioned, with regards to homogeneity, that countries will have to decide whether such harmonization has to come in the form of regulation or as soft-law.

8. Should the UDRP have financial damages awarded, both for complainants and respondents?

Malcom Bain highlighted that a company may get financial damages if launches a court case, but there is no financial damages award on the UDRP procedure. As such, albeit it could put

arbitrators in a difficult position deciding on damages and costs, it could be a deterrent for cyber-squatters and potential infringers.

Caroline Berube outlined that there should be financial compensation, but its effectiveness may depend on the individual idiosyncrasies of a particular market. In China, there is a sizeable number of cyber-squatters, therefore even if there is an award granting financial compensation, it could be difficult to actually receive such compensation from the infringer.

9. What are the main issues arising from the registration of trademarks and domain names consisting of a family name?

Malcom Bain exposed that there are some country specific provisions governing this type of cases, because while other jurisdictions may pose problems to domain name registration of surnames, in Spain you can register your name/surname as a domain name - the only thing you cannot do is registering someone else's surname as a trademark. The issue with this may be that some trademark laws establish that you cannot prevent someone else using their own family name (which could be the same as yours) - including within a domain name, therefore.

Ruben CANO PÉREZ

Fide and TIPSA (Transatlantic Intellectual Property Academy) join forces to organize a serial of digital encounters to try and find out if Intellectual Property is equipped to face the ongoing changes that our world is experiencing.

All online encounters are opened to any interested person and speakers have been selected among the most relevant IP scholars and professionals all over the world.

The Global Digital Encounters form integral part of the solidarity projects run by both organizations to support the international, European and national plans to overcome the sanitary and financial consequences of the COVID-19

