SCC Online Web Edition, Copyright © 2020
Page 1 Thursday, September 03, 2020
Printed For: Dr. Amandeep singh, Dr. RML National Law University
SCC Online Web Edition: http://www.scconline.com

10 RMLNLUJ (2018) 218

Liability of Domain Name Registrars

by
Pallavi Khanna[*]

ABSTRACT

The aim of this paper is establish a framework where the obligations and responsibilities of the registrar in relation to domain name disputes can be clearly prescribed. The objective underlying this study is to understand the circumstances where liability issues may arise in cases relating to registration of domain names and how the current legal framework seeks to address these concerns. The scope of the paper encompasses aspects such as the problems relating to domain names with respect to role of registrars as intermediaries, competition law issues arising in domain name registration and how courts have interpreted the liability of registrars internationally. The paper is restricted to analyzing the current position in India with respect to issues in classifying them as intermediaries and assessing the anti-competitive practices in registration, initiatives by ICANN, examination of judicial approach in the US and an overview of arguments for and against imposing liability on registrars. Technical and procedural aspects such as mode of registering domain name, trademark infringement aspects, cyber-squatting issues in India, etc. is excluded from the purview of this paper. Thus the author seeks to answer questions such as-What is a domain name? Why do we need to protect domain names? How do registrars limit their liability? What is the extent to which registrars should be held liable and in what circumstances? Does India have effective measures to adequately address problems relating to domain name registrations? Can domain name registrars be called intermediaries? What are the competition law issues arising with respect to domain name registration? How has the US dealt with problems arising in relation to liability of domain name registrars?

Keywords: Domain Registration, Registrars, Intermediaries, Infringement, Competition Law, Liability Issues, Unfair Practices, IPR

I. INTRODUCTION

Whenever a website is set up, the primary step is to register a domain name for it. A domain name refers to the unique address guiding the browser of the user to the computer where the website resides. Since every internet resource such as web pages has an address of its own, called the URL; or the Uniform Resource Locator, the domain name forms a part of the address that is assigned to every computer or internet service. The domain name system links the names to a number series or IP address and these numbers are linked with an easily understood address called the domain name. The ICANN (Internet Corporation for Assigned Names and Numbers) and WIPO (World Intellectual Property Organization) have prescribed stringent measures such as a rigorous method of registering domain names with only those registrars accredited by ICANN on a first come first served basis.[1]

The role of domain names was initially confined to giving an address for computers

SCC Online Web Edition, Copyright © 2020
Page 2 Thursday, September 03, 2020
Printed For: Dr. Amandeep singh, Dr. RML National Law University
SCC Online Web Edition: http://www.scconline.com

but govern the development of the internet from a channel of communication to a means of commercial activity, domain names are also used as business identifiers. Domain names are accessible irrespective of the geographical location of users. This not only implies that there is a need for worldwide exclusivity but that the domestic laws might be insufficient to protect domain names.[2]

Domain name protection has been overdue in India since a while now. Since there is no dedicated law for domain name protection, they are

generally dealt with under the Trademarks Act, 1999 since they have the same characteristics as trademarks. Hence infringement actions have been initiated in case of domain names that are registered trademarks. The courts have also been forthcoming in granting orders against infringing domain names. Thus the entities authorised to provide domain name registration services are called registrars and registration with such registrars serves as an evidence of recognised user of a mark even if it does not have the same consequence as registration as a trademark. The registration is guided by the Uniform Domain Name Disputes Resolution Policy (UDRP) and disputes against the registrant may be referred to dispute resolution service providers recognised by ICANN.[3]

II. COMPETITION LAW ISSUES IN DOMAIN NAME REGISTRATION

The domain name registration market is very competitive and the top 20 registrars tend to account for more than 75% of a market. Go Daddy is the leading registrar with maximum share of registrants.[4] It is the trademark infringement cases which often see claims of unfair competition being made as well.[5] Registering domain names to disrupt the competitor's business is also an act of cyber-squatting. In fact in Japan, cyber-squatting has been explicitly identified as an unfair competition act in the Unfair Competition Prevention Law in 2001. The Beijing High Court has also recommended that the Anti-Unfair Competition Law should be applied to address issues of malicious registration of domain names.[6]

Competitive Registration Process

The domain name registration process is less stringent than registering trademarks since it is based on a first come first served basis. In a study a few years ago, it was seen that out of the 860 ICANN accredited registrars, 533 belonged to the US and 83% of the total revenue arising from domain registration went to the US. Majority of the root name server operations and gTLD registry operators were based in the US as well. This along with the slow response time of root servers across several locations implied that

other regions were underserved and hence in these circumstances, having a first-come-first-served (FCFS) policy for registering domain names is unfair towards registrants who belong to under-served regions. We need to devise a more effective policy for domain name infrastructure.[7]

The FCFS system further permits registrants who have no connection with a domain name or remote connection to get allocated a domain name linked to a popular brand and they can later sell it for ransom to those who have close linkage with the name in

SCC Online Web Edition, Copyright © 2020
Page 3 Thursday, September 03, 2020
Printed For: Dr. Amandeep singh, Dr. RML National Law University
SCC Online Web Edition: http://www.scconline.com

question. Hence this means unauthorised registrars try to profit from the goodwill of trademark owners. This is problematic since there can be one domain name only, unlike trademarks which may be multiple in number for different spheres. This creates more trouble when the domain names are put for auction by registrants.[8]

The growth of internet has enhanced instances of counterfeiting and those of trademark infringement which take place through online forums. Resemblance of domain names adversely affects the growth of market of the original domain name in question since it causes direct competition by deceiving the consumers and inducing them to assume that the infringing trademark is the same as the original domain name.

In one instance, the court found that a domain name registrar had registered around 663 domain names which infringed the mark of Verizon Communications by using alias registrants. It was found that the use of aliases, trend of domain name kiting and infringement reflected bad faith and intentional infringement.[9]

Those in favour of enhancing the liability of the registrar argue that, given the increasing rate of instances of cybersquatting in India, registrars must make concerted efforts to address this issue at the level of registration by examining the claims of the persons seeking registration of the domain name and by doing background checks rather than adopting a blind approach of allocating domain names.[10]

Although many domain names are available for registering, by preventing an entity from using the name that connotes its product by preventing use of the trademark it owns, puts them at a huge competitive

disadvantage.[11] Even digital domain name registrars have acknowledged the difficulty in accessing customers outside their domestic market.

Tricks employed by Registrars

These days everyone is in need of a website and every website requires a domain name as well as a hosting server. In most of the cases, the same company is the one providing the domain registration and the hosting service. There are as many as 50,000 websites that are launched every week and those many companies are striving to attract customers. This manifests in the form of cutthroat competition between web hosting companies and hence a number of unfair practices are a common feature. Though competition is healthy for business, this kind of competition has crossed ethical boundaries and the registrars use every kind of method to extract as much money from the registrant. Taking a domain is an easy exercise but preserving it for an extended time is not easy, especially when the domain becomes famous and its demand in the market increases. Unlike hosting servers, domain names are not easy to change. Any alteration in the domain name might entail transforming business strategies, losing a customer base, changing emails and even identities in a number of places. There are times where the company has to spend a significant amount of money fighting legal battles just to retain the domain name.[12]

Sometimes, there are deceptive advertisings which show discounts on domain names to show that they have become cheaper. However subsequently what happens is that the registrant will usually have to pay a higher price if he wishes to renew it in the next year. Hence the advantage of buying it cheap in the first go is nothing but a farce. All registrars attempt to hound customers of other registrars by giving cash benefits ad discounts such as one year free. This doesn't actually mean that the registrant will get the domain free for another year but that they will not lose out on

SCC Online Web Edition, Copyright © 2020
Page 4 Thursday, September 03, 2020
Printed For: Dr. Amandeep singh, Dr. RML National Law University
SCC Online Web Edition: http://www.scconline.com

the leftover life of their domain. Though some domains can be registered for more than a year, an advance payment is needed. Moreover, some may ask for credit card details and many unsolicited deductions are made from the card though your domain name payment will be completed. Moreover the refund offers are linked to hosting polices. The registrar may pay the registry part of the sum paid but the registrant and then again registrant is asked to renew it in the next year. Also, to attract more registrants, the registrars even offer the transfer prices at a lower rate than the price for purchasing or renewing the domain. This is problematic for those wishing to continue because the domain charges are generally higher with each year

and renewal charges are greater than new domain charges, domain which was earlier free with the hosting now has to be paid for and the hosting package also increases. Since the intimation about the higher charge to renew is received only a month before the expiry, it leaves very little time for the registrant to transfer the domain. Domains expire if there are delays in renewal but if the registrar keeps it on hold for around a month, he extracts an additional fee from the registrant following which the domain enters a redemption period where the registrant has the last chance to get the domain renewed and is very costly in comparison to the original registration. The hosting companies who also offer registration services try to lure customers by charging a high price for hosting which is usually much higher than the average cost of registration but also provide a 'free' domain name along with the hosting service. This helps in retaining customers for the whole year since they are asked to comply with a number of conditions to avail the package. Similarly, domain registrars often present a long list of services that they provide such as DNS configuration, updating who is record, multiple email addresses to redirect mails received by the domain, domain parking, private registration to protect against spam, automatic configuration with Google services, etc. In this long list, configuration, redirection and updating who is done by all the registrars. Email forwarding is required by some registrants for a temporary period only and other services are rarely useful. Hence the customers are easily attracted to register when they see that so many services are being provided, without evaluating if they actually need those services for their individual needs. Most registrars also promise that they will give 24×7 customer service though in practice they may not be always available through email/ live chat/ telephone, etc. Usually the domains are such that no support from the registrar is actually needed. However, if the domain control interface is not working properly then support from registrar may be needed. But this is a basic service which the registrar should not charge extra for in the garb of 2487 customer support, especially when only automated replies are received and actual help is offered much later.[13]

Recourse available to registrants

Due to the tricks adopted by registrars to trap more customers, the ICANN has set out a policy governing the transfer of registrations. It requires you to remain with a domain for at least 60 days before transferring it, the new domain cannot have a new email, the status of the domain has to be unlocked before transferring, the old registrar needs to provide an authorisation code to the new one, all registrars are not permitted to transfer all kinds of addresses, etc. These regulations were important to restrict mass transfers and avoid any registrar to gain by unfair practices. However,

SCC Online Web Edition, Copyright © 2020
Page 5 Thursday, September 03, 2020
Printed For: Dr. Amandeep singh, Dr. RML National Law University
SCC Online Web Edition: http://www.scconline.com

even these have been misused by the registrars. For instance, they may lock the domain prior transfer and not assist with unlocking. Even after the registrant unlocks it without the aid of the registrar or with administrative help, the domain is kept locked internally to delay the transfer process and disrupt transfer. They may also keep delaying revealing the authorisation key if the registrant is unable to secure it with the control panel. They also refrain from assistance when the domain is acquired by a reseller. It is advisable for the registrant to have different companies for hosting and registration of the domain name so it is easier to change the server.[14]

The registrants can complain in case domain related problems arise but lack of awareness with respect to the procedural rules causes problems and it is a very time consuming process. In addition to this, the high level of competition for high profits creates further gaps between the players in the industry. Though the bigger companies charge more for surviving, even smaller companies tend to be greedy and extract more at later stages even if it involves crossing ethical boundaries for profits. Some entities even make money not by selling the domain names but by parking and then selling them at a higher rate.[15]

Passing Off

The concept of passing off can be applied to different kinds of unfair trading where conduct of one party can injure the goodwill of another entity. Passing off is said to be an unfair trade practice since one person tends to achieve an economic benefit of another's reputation by deception.[16] Competition law issues are encompassed by the tort of passing off as well. It occurs when a trader misrepresents his goods to customers by making them confused and assumes they are buying goods of a particular brand. The bad faith registration of a domain name makes the registrant liable for passing off. This takes place when the registrant registers the domain name for selling, renting or transferring the registration of the domain name to the complainant who owns the trademark or his competitor at a very high cost. Since this pertains to the liability of the registrant and not the registrar, it is outside the scope of this paper.[17]

III. INTERNATIONAL FRAMEWORK FOR REGISTRAR LIABILITY

ICANN

At the international level, ICANN manages the dispute resolutions relating to domain names under the Uniform Domain Name Disputes Resolution Policy of 1999. Article 2 imposes a duty on the registrar to not register domain names for unlawful reason and to not use it knowingly in contravention of any law. It also mandates a registration agreement that prohibits website from being used for unlawful activates and the registrar is contractually required to shut it down. However, the registrar can evade liability if they had no knowledge of the illegal information.[18]

Approach in the United States

In the US, the problems related to domain name registration are better addressed than in other jurisdiction. Though infringement claims are usually directed towards registrants, in the US some cases focus on the liability of registrars in these instances as well.

The Anti-cybersquatting Consumer Protection Act of 1999 (ACPA) seeks to create a

SCC Online Web Edition, Copyright © 2020
Page 6 Thursday, September 03, 2020
Printed For: Dr. Amandeep singh, Dr. RML National Law University
SCC Online Web Edition: http://www.scconline.com

mechanism for combating infringing domain names. There has been a trend, witnessed in the US, that to qualify as a contributory infringer, there must be knowledge of infringement or some assistance must have been given to facilitate the infringement. Usually the courts have denied the liability of registrar in these suits.

The ACPA doesn't intend to shield registrars from liability when they are acting outside of their core functions as registrars and are faulting in providing other services such as in the provision of privacy services[19] or when it is generating revenue from a parked pages program.[20] Hence the status of a registrar is not an immunity when it is not acting as a registrar only.

In *Lockheed Martin*[21], the suit for contributory infringement failed since the registrar's role was limited to registration and it was held that they

cannot be expected to supervise the internet to ensure no infringement is taking place. Hence the registrar only performs the role translation service by converting the domain name into an IP address.

GoDaddy, a domain registrar, was sued for violating the ACPA for infringement of domain names on the grounds that it was monetizing by use and trafficking of the domain name that was identical to the Academy's trademarks. The parked pages program, unlike the domain registration program allowed GoDaddy to generate revenues by registering the domain name. While GoDaddy sought immunity under the safe harbour protection of the ACPA which requires a bad faith intent to profit from registration, this claim was struck down since it favours only those who are acting in the registration or maintaining capacity only but because GoDaddy had placed ads on the parked webpages for generating revenue and were licensed by the registrant, they were actively involved in trafficking and use of the domain name. Hence since the function was not limited to acting as a registrar, GoDaddy was held liable for contributory infringement of the domain names.[22]

However, in another case against GoDaddy itself, the platform was used to forward the visitors of a domain name Petronas to porn sites. It was held that imposing a secondary liability on the registrar will unnecessarily expand the ambit of the ACPA to cover those who are not cyber squatters but who's actions may facilitate it and hence cover even those who have no bad faith and are merely responsible for maintenance. Here since the registrar was not exercising any direct control on the cyber-squatting as it was merely routing the users, it did not amount to contributory cyber-squatting and hence secondary liability was not imposed on the registrar.[23] This was a welcome judgement since it exempts those who are not using the domain name for cyber-squatting and it also spares the registrars the agony of predicting the intention of their customers while registering domains.

In *Register.com* v. *Domain Registry of America Inc.*[24], a case was filed alleging an unauthorised transfer of the domain name registrars. The complainant claimed that the competing registrar, the defendant, was slamming the customers of the plaintiff by marketing tools that were unfair. The defendants sent several communications immediately prior to expiry of the customer's domain name registration with the plaintiff. This resulted in confusing and misleading consumers about the nature of services as well as the origin of the defendant. They unwittingly switched their domain registrar

SCC Online Web Edition, Copyright © 2020
Page 7 Thursday, September 03, 2020
Printed For: Dr. Amandeep singh, Dr. RML National Law University
SCC Online Web Edition: http://www.scconline.com

while assuming they are renewing their agreement through the defendant which is an authorised reseller of a competing registrar. An injunction was granted for the anti-competitive practices since the 'renew' option tends to imply that the mail is from the existing registrant and not a new competing registrar. Hence it confused registrants about it being their existing registrar or an affiliate to assist with their registration. Evidence of a disproportionate number of transfer requests initiated through the defendant showed that the customers were confused by the defendant's advertisements. Thus preliminary injunction was granted for the unfair trade practice.

Approach in the European Union

In the European Union, the registrars are immune from liability unless they have the knowledge that the website they host is engaging in unlawful activities. Article 14 of the Directive 2000/31/EC[25] states that the registrar should be unaware of the illegal activity or information and must promptly remove it when he becomes aware of it.[26] The author opines that this would be applicable to WikiLeaks since every domain registrar is contractually obliged through the registration agreement to shut websites engaging in criminal activities such as publishing classified government information.

Interestingly, Germany held Key Systems, a domain registrar, liable for infringement of copyright since it issued a domain name to a hacker and did not take it down despite receiving sever notices of the unlawful activity. This was the first time that instead of the website operator, it was the domain registrar who was being held liable.[27]

Also, when a registrar offered a number of domain names which were similar to established trademarks, the bad faith intent of the registrar to confuse the customers was evident. The registrar was also profiting from the privacy services and the monetization schemes in addition to shielding registrants from liability.[28]

However in another French case, the registrar was not held liable because it was held that putting the burden of screening domain names and see if trademark being infringed is an unreasonable expectation from the registrar and he doesn't have the skill set to carry out this kind of a monitoring on their own.[29]

It has been held that the test to determine the liability of the registrar is that it should be proved that he had knowledge that it was not advisable to register the domain name.[30]

IV. DOMAIN NAME REGISTRARS AS INTERMEDIARIES IN INDIA

After the amendment of Section 2(w) of the Information Technology Act, 2000 in 2008, the definition of an 'intermediary' has been expanded and it seems that it seeks to imply that all intermediaries part of online transactions will be regarded as intermediaries under this act.[31] Though the Act doesn't specifically mention domain name registrars in the definition, since they are sometimes involved with the storing and transmitting of information and provide services of registration in relation to the records, it can be said that they are also intermediaries but this will again depend on the role the registrar is performing and the extent of control he exercises. If it is merely registration and he is not involved with the supervision of content on a registered domain, his liability must be differentiated from that which falls upon an intermediary.[32]

SCC Online Web Edition, Copyright © 2020
Page 8 Thursday, September 03, 2020
Printed For: Dr. Amandeep singh, Dr. RML National Law University
SCC Online Web Edition: http://www.scconline.com

Moreover, it is also argued that registrars act as intermediaries between the local domain name authority or registry and those seeking to register their domain names.[33] This has been observed in some international cases as well since registrars assist in registration and transfer of domain names.[34] Registrars have been classified as intermediaries under the OECD (Organisation for Economic Co-operation and Development) as they facilitate and bring together transactions between third parties online.[35]

Hence, if the registrar's acts are similar to an intermediary and not limited to mere registration, he should be entitled to the safe harbour protection

under Section 79 of the Information Technology Act, 2008 (IT Act) when he can show lack of knowledge of offence committed by third parties and when he undertook proper due diligence in registering the domain name.[36]

The National Stock Exchange also made claims for copyright infringement against GoDaddy. It was observed that GoDaddy would be liable as an intermediary under Section 2(1)(w) of the IT Act since it includes web hosting services however it is entitled to protections available under section 79. However, what is problematic is that the term ‘knowingly’ is ambiguous. The capacity to monitor content will depend on the operating intermediary. Section 2(1)(w) though encompasses web hosting services as well, don’t recognise that the liability may be hard to establish. This is because supervision of large amount of content and subjective nature of monitoring that is needed to ascertain if any infringement is taking place requires judicial application of mind which, the author opines, is an enhanced burden on the registrar who's original duty of registration of domain name should not be extended. Exercising such supervision over millions of pages of the domain names it registers is impossible to do and it may result in pre censorship by the registrar.[37]

Recently, a domain registrar blocked the website of a cartoonist on a complaint of contravention of the Penal Code, 1860 on a notice was sent by the Mumbai Police to the domain registrar which then went ahead and removed the domain. Domain registrars often receive complaints for content screening according to the regulations prescribed. It has been recognised that intermediaries such as Big Rock are required to incorporate a number of grounds in their customer service agreement when they are acting beyond their capacity as a registrar alone.[38]

An Internet Service Provider refers to a business or organisation offering users access to Internet and associated services. Most telecom operators qualify as ISPs since they extend services such as internet transit, dial up, registration of domain names, etc. It's important to note that the liability is not contingent on what an entity is but what is does while transmitting information.[39] It has been said that the role of the domain name registrar in the internet can be distinguished from an internet service provider who is actually responsible for the storage and communication of infringing material.[40] Hence, while determining if a party can be made secondarily liable for contributory infringement, one must focus on the extent to which it can

SCC Online Web Edition, Copyright © 2020
Page 9 Thursday, September 03, 2020
Printed For: Dr. Amandeep singh, Dr. RML National Law University
SCC Online Web Edition: http://www.scconline.com

control and supervise the activities of the infringing party.[41]

Hence, in the digital world, there will be some classes of intermediaries such as the ISPs who carry data but do not exercises any kind of direct control on the content, though they may have the potential to exercise control. Keeping in mind the drive to promote electronic transactions, it is crucial to clarify, and when necessary, to limit the liability of these intermediaries. It is suggested that intermediaries such as registrars and network service providers should not be made responsible for content of third parties for which they are merely providing access.

V. DEBATES SURROUNDING LIABILITY OF REGISTRAR

What happens in a lot of circumstances is that the registrar is compelled to take the domain down. However this isn't a cure since the forum owner just ends up opening shop under another registrar, like it happened in the

case of *Pirate Bay*. Before suing the registrar, the domain name owner should be conversant with the terms of use set out in the registration agreement. The terms of service generally state that the registrar will ensure the user information is confidential and will not be shared with third parties without their consent. Registrars also exempt themselves from personal liability. Though the registrars sometimes also state that they have the right to pre-screen the content to check if it's appropriate, this is not the norm and it will determine the extent to which claims against them can be made depending on the amount of control they exercise over the matter.

Need for making registrar liable

The role of the registrar has changed considerably and it is possible that have actual knowledge that the registration was done in bad faith.[42] This is why in UDRP proceedings as well, the registrar is notified that there has been a complaint against its customer so that the domain name is locked down and not transferred during pendency of proceedings. The registrar is also supposed to transfer the domain name to the complainant if the trademark complaint succeeds.[43] It has also been said that registrars are supporting counterfeiting and facilitating piracy by refusing to comply with the ICANN rules that seek to foster legitimate activities on the internet.[44] The era of registrars having a blanket immunity is over. In order to extend liability to registrars, it has been held that even registering of a domain name is an act that by itself may be viewed as being a commercial act since it involves a sale which takes place between the registrant and registrar, thus falling within the ambit of 'use in commerce' as mandated by the law.[45]

Heightening the liability of registrars providing registration services for regular violations will be a welcome move for consumers and brand owners. Though registrars have policies authorising them to terminate the accounts of customers.[46] if they are violating rights of others, the registrars are usually reluctant to enforce these measures because of a lack of incentives since he will lost out on customer base as the customer will merely move elsewhere thereby causing competing disadvantage to the registrar. Moreover, some registrars are cyber-squatters themselves or exist solely

for supporting cyber-squatters[47]. Hence a high legal standard will create a level playing field and will be effective if it is supplemented with better incentives for good

SCC Online Web Edition, Copyright © 2020
Page 10 Thursday, September 03, 2020
Printed For: Dr. Amandeep singh, Dr. RML National Law University
SCC Online Web Edition: http://www.scconline.com

practices in order to evict bad actors. Registrars can also include a provision for indemnification in their policy if they are made secondary liable for instance when they don't terminate the account of the scrupulous registrants.[48]

Arguments against the liability of the registrar

Registrars, in their given capacity, are mere conduits registering domain names and do not qualify as registrants or licensees and hence qualify for protections available to registrars. Hence, the courts have distinguished the liability of registrars when they merely process requests for registering domain names from that of the registrant who may be held responsible for acts of cyber-squatting by virtue of 'use' of the domain name.[49] The domain registrar is a part of the bigger infrastructure powering the Internet. When this agency starts being policed, then it will turn them into law enforcement agents, a task they are not always able to handle. If registrars begin taking down the domain names on receiving notifications from third parties then it will open the floodgates of litigation with the registrar soon becoming strictly liable. Nevertheless, it is important to ensure that this is not used by a means for them to shirk their responsibilities in regulating undesirable matter. Hence, the laws should clearly state that though registrars will not be liable for third party data, they will not be absolved form their obligations in terms of removal of content when asked.

VI. CONCLUSION AND RECOMMENDATIONS

Though the IT Act addresses a number of cybercrimes and has even been forward in its thinking by mandating the set up of cyber crime cells, the Act has neglected to address the issue of domain name disputes and that of cyber-squatting. The only recourse available to the victims of these offences is that domain names are considered trademarks on the basis of their use and reputation of the brand, hence subject to the Trade Marks Act of 1999. Judicial decisions have acknowledged issues arising from domain names and have tried to address them with the use of injunctions, transfers and even by awarding damages under passing off.[50]

Since the law pertaining to online market places and those pertaining to secondary infringement of trademarks are still at a nascent stage, it makes it difficult for courts to take concrete steps. Harassment, interest confusion, illegal gains, free riding on goodwill are a part of the domain name disputes and need the attention of the legislature, administrative bodies and the judiciary. If India is unable to prioritize this issue, it should respect and put in effect the ratified international laws and procedure. The immediate need is though for the legislature to amend the IT Act 2000 and provide for cybersquatting and domain name disputes. India can also take inspiration from the US in following a model similar to that envisaged under the ACPA.

In the opinion of the author, it is not reasonable or commercially viable for domain name registrars to verify the veracity of all domain names being registered and the purpose for which they are used. Given the borderless world of the internet, it is important to have a uniform standard on the concern of secondary liability for trademark infringement done online. The creators of harmful content should have more responsibility than intermediaries or registrars. The internet should not become a forum where the law enforcers area able to determine who can register a domain name. Registrars, if assigned with the duty of monitoring content, will transform into cyber-police while blindly adhering to the requests of the law enforcement agents. This

SCC ONLINE
The surest way to legal research!
SCC Online Web Edition, Copyright © 2020
Page 11 Thursday, September 03, 2020
Printed For: Dr. Amandeep singh, Dr. RML National Law University
SCC Online Web Edition: http://www.scconline.com

may pose serious threats to the idea of net neutrality. The liability of the registrar should be restricted and exceptional. Making registrars liable for the acts of their users will suppress innovation because companies will be compelled to hire legal teams to investigate possible infringements and such a heavy obligation may deter registrars because of strict licensing. This may also mean that registrars will block domain names erroneously fearing liability. Hence it restricts their freedom to do business when required to assess infringement cases. It would be better if they are instead asked to respond to removals ordered by courts so that it eliminates the need for analysing all claims.

---

* Law Clerk-cum-Research Assistant, High Court of Delhi, Delhi. <pallavi.nls17@gmail.com>

[1] Nishith Desai Associates, E-Commerce in India July 2015 Legal, Tax and Regulatory Analysis, (July 2015) *available at* http://www.ivca.in/reports/2015/India_E_Commerce_Report_Nishith_Desai_Associates.pdf (accessed February 3, 2017).

[2] Hemant Goyal, Mohit Porwal, "India: Protection of Domain Name as a Trademark", (July 14, 2014), Mondaq, *available at* http://www.mondaq.com/india/x/327272/Trademark/Protection+of+Domain+Name+As+A+Trademark (accessed February 4, 2017).

[3] *See Satyam Infoway Ltd.* v. *Siffynet Solutions (P) Ltd.*, (2004) 6 SCC 145 : AIR 2004 SC 3540. Also see *Yahoo Inc.* v. *Aakash Arora*, 1999 SCC OnLine Del 133 : 1999 PTC 201 and *Rediff Communication Ltd.* v. *Cyberbooth*, 1999 SCC OnLine Bom 275 : AIR 2000 Bom 27.

[4] OECD, "The Economic and Social Role of Internet Intermediaries", (April 2010) *available at* https://www.oecd.org/internet/ieconomy/44949023.pdf (accessed February 3, 2017).

[5] *Panavision International LP* v. *Toeppen*, 141 F 3d 1316 : 46 USPQ 2d 1511 (CA 9 1998).

[6] Guidance Opinion, Art. 4 issued by the Beijing High Court on August 15, 2000: The Malicious registration of another person's or company's famous mark as one's domain name violates principles of good faith and commercial ethics, and constitutes unfair competition.

[7] Prof. Vandana. Narvade. Kadam, "Analytical Study of Domain Name System, its Disputes and Legal Issues", BVIMSR'S Journal of Management Research, 19, (April, 2013).

[8] *Supra* note 2.

[9] *Verizon California Inc.* v. *OnlineNIC Inc.*, 647 F Supp 2d 1110 (2009).

[10] Zohaib Hasan Khan et al, "Cybersquatting and its Effectual Position in India", 6(2) INTERNATIONAL JOURNAL OF SCIENTIFIC ENGINEERING RESEARCH, 880, (February 2015).

[11] G.B. Dinwoodie, "(National) Trademark Laws and the (Non-National) Domain Name System", University of Pennsylvania Journal of International Economic Law, 505 (2000).

[12] U. Mishra, "Dirty Tricks Played by the Domain Registrars", SOCIAL SCIENCE RESEARCH NETWORK *available at* http://ssrn.com/abstract=1974978.

[13] *Ibid.*

[14] *Ibid.*

[15] *Ibid.*

[16] Jagadish A.T., "A Critical Study on Menace of Cybersquatting and the Regulatory Mechanism", ISSN 2321-4171, (2014).

[17] "What are the Rights of a Trademark Owner?", MANUPATRA.

[18] Uniform Domain Name Dispute Resolution Policy, Internet Corporation for Assigned Names & Numbers 7 (October 24, 1999) *available at* http://www.icann.org/en/help/dndr/udrp/policy (accessed February 4, 2017).

[19] *Solid Host, NL* v. *NameCheap Inc.*, 652 F Supp 2d 1092, 1106 (CD Cal 2009).

[20] *Transamerica Corpn.* v. *Moniker Online Services, LLC*, 672 F Supp 2d 1353, 1366 (SD Fla 2009).

SCC ONLINE
The surest way to legal research!
SCC Online Web Edition, Copyright © 2020
Page 12 Thursday, September 03, 2020
Printed For: Dr. Amandeep singh, Dr. RML National Law University
SCC Online Web Edition: http://www.scconline.com

[21] *Lockheed Martin Corpn.* v. *Network Solutions Inc.*, 194 F 3d 980 (9th Cir 1999) and S. 1125(*d*)(2)(D)(*ii*) ("The domain name registrar or registry or other domain name authority shall not be liable for injunctive or monetary relief under this paragraph except in the case of bad faith or reckless disregard, which includes a wilful failure to comply with any such court order.").

[22] *Academy of Motion Picture Arts and Sciences* v. *GoDaddy.com Inc.*, 2015 WL 5311085 (CD Cal September 10, 2015).

[23] *Petroliam Nasional Berhad* v. *GoDaddy.com Inc.*, 737 F 3d 546, 548 (9th Cir 2013).

[24] Case No. 0206925 (NRB) Southern District of New York, December 27, 2002.

[25] Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that: (*a*) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or (*b*) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

[26] H. Murphy, "Thesis: The Role of a Domain Name Registrar as an Internet Intermediary" — Tilburg University.

[27] *Universal Music* v. *Key-Systems GmbH* [2014] Regional Court of Saarbrücken http://classactionaction.com/domainnameregistrarsandlawenforcement/.

[28] *Verizon California Inc.* v. *Above.com Pty. Ltd.*, 881 F Supp 2d 1173 (CD Cal 2011).

[29] Association Francaise pour le Nommage Internet en Coopération Paris Court of Appeal, October 19, 2012 (EuroDNS).

[30] *Ford Motor Co.* v. *GreatDomains.com Inc.*, 177 F Supp 2d 635 (ED Mich 2001).

[31] Ammu Charles, "Online Auction Sites: Liability for Counterfeit Goods", (2015) 6 SCC J-3.

[32] *Infra* note 48 at 3.

[33] Bent Petersen, Lawrence S. Welch, "International Business Development and the Internet, Post-hype", 43(1) MIR: MANAGEMENT INTERNATIONAL REVIEW, 7 (2003).

[34] *Office Depot Inc.* v. *Zuccarini*, 596 F 3d 696 (9th Cir 2010).

[35] OECD, The Economic and Social Role of Internet Intermediaries, 9, (2010), *available at* https://www.oecd.org/internet/ieconomy/44949023.pdf (accessed February 4, 2017).

[36] S. 79, Information Technology Act, 2000:

> "Intermediaries not to be liable in certain cases
>
> (1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-ss. (2) and (3), an intermediary shall not be liable for any third-party information, data, or communication link made available or hasted by him.
>
> (2) The provisions of sub-section (1) shall apply if—
>
> (*a*) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hasted; or
>
> (*b*) the intermediary does not—
>
> (*i*) initiate the transmission,
>
> (*ii*) select the receiver of the transmission, and
>
> (*iii*) select or modify the information contained in the transmission;
>
> (*c*) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.
>
> (3) The provisions of sub-section (1) shall not apply if—
>
> (*a*) the intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of the unlawful act;

SCC Online Web Edition, Copyright © 2020
Page 13 Thursday, September 03, 2020
Printed For: Dr. Amandeep singh, Dr. RML National Law University
SCC Online Web Edition: http://www.scconline.com

(*b*) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

Explanation.—For the purposes of this section, the expression "third-party information" means any information dealt with by an intermediary in his capacity as an intermediary".

[37] Thomas J. Vallianeth, "GoDaddy to be Sued as an Intermediary for Copyright and Trademark Infringement", (April 21, 2014), SpicyIP, *available at* https://spicyip.com/2014/04/godaddytobesuedasanintermediaryforcopyrightandtrademarkinfringement.html (accessed February 4, 2017).

[38] A. Gupta, "Cartoons Against Corruption : How the Law Aids Web Censorship", India Law and Technology Blog *available at* http://www.iltb.net/2012/01/cartoonsagainstcorruptionhowthelawaidswebcensorship/.

[39] Ahmad Kamal, United Nations Institute for Training and Research, *The Law of Cyber-Space: An Invitation to the Table of Negotiations*, (October, 2005) *available at* https://www.un.int/kamal/sites/www.un.int/files/The%20Ambassador's%20Club%20at%20the%20United%20Nations/publications/the_law_of_cyber-space.pdf (accessed February 4, 2017).

[40] *Gucci America Inc.* v. *Hall & Associates*, 135 F Supp 2d 409 (9th Cir 1996).

[41] *Infra* note 50, at 5.

[42] Wendy C. Larson, "Internet Service Provider Liability: Imposing a Higher Duty of Care", 37 COLUMBIA JOURNAL OF LAW & ARTS, 573, (2014).

[43] *Supra* note 36.

[44] William New, Annual USTR Notorious Markets Report Points Fingers, Includes Domain Registrars for First Time, INTELLECTUAL PROPERTY WATCH, (2015) *available at* http://www.ip-watch.org/2015/03/06/annual-ustr-notorious-markets-report-points-fingers-includes-domain-registrars-for-first-time/ (accessed February 4, 2017).

[45] *Jack in the Box Inc.* v. *Jackinthebox.org*, 143 F Supp 2d 590 (EDVa 2001).

[46] *See, e.g.*, *Register.com Master Services Agreement*, Register.com (January 28, 2014), http://www.register.com/policy/servicesagreement.rcmx.

[47] *Dell Inc.* v. *Belgium Domains*, LLC, 07-22674-CIV, 2007 WL 6862342.

[48] *Infra* note 50 at 576.

[49] *Solid Host, NL* v. *NameCheap Inc.*, 652 F Supp 2d 1092 at 1105 (CD Cal 2009).

[50] Christine Chiramel, "The Domain Name Chaos — A Legal Perspective", (August 19, 2011), Mondaq, *available at* http://www.mondaq.com/india/x/142874/Trademark/The+Domain+Name+Chaos+A+Legal+Perspective (accessed February 4, 2017).

Disclaimer: While every effort is made to avoid any mistake or omission, this casenote/ headnote/ judgment/ act/ rule/ regulation/ circular/ notification is being circulated on the condition and understanding that the publisher would not be liable in any manner by reason of any mistake or omission or for any action taken or omitted to be taken or advice rendered or accepted on the basis of this casenote/ headnote/ judgment/ act/ rule/ regulation/ circular/ notification. All disputes will be subject exclusively to jurisdiction of courts, tribunals and forums at Lucknow only. The authenticity of this text must be verified from the original source.