TRADEMARK TRAFFICKING IN CYBERSPACE: AN ANALYTICAL STUDY

SUMMARY OF THESIS
Submitted to the
Faculty of Laws
PANJAB UNIVERSITY, CHANDIGARH
for the degree of

DOCTOR OF PHILOSOPHY

2011

RAJIV BHALLA
Department of Laws
Panjab University
Chandigarh
TRADEMARK TRAFFICKING IN CYBERSPACE: AN ANALYTICAL STUDY

Summary of Thesis Submitted to the
Faculty of Laws,
Panjab University, Chandigarh

RAJIV BHALLA

Domain Names are being increasingly considered prized possessions by individuals and organisations, which have a goodwill associated with their name, trade name, or trademark, to protect. Therefore, it is incumbent upon legal and administrative machinery to protect the legitimate interests of the stakeholders without encroaching on anyone’s right of free speech and fair use of Internet addresses.

Besides domain names, trademarks in cyberspace are also under threat due to innovative use of technology in the form of Meta tags, Search Engine advertising, pop-ups, spam, links, frames, and mousetrapping. Though to a lesser extent, yet these issues cannot be overlooked while striving for an effective redressal system for alleged trademark violations in cyberspace.

The pivotal role played by Search Engines, like Google, Yahoo, MSN, Bing, etc. in driving Internet traffic to the websites the surfers are looking for, is largely responsible for ever-increasing instances of trademark trafficking in cyberspace. With the success of a website directly linked with the number of visitors it can attract, there is frenzy among the existing and prospective website owners to popularise their web address among Search Engines even at the expense of violating established trademark principles that prevail in the real world.

As Internet emerges as a frontline platform for conducting business, with e-commerce being buzzword in trading circles, the monetary incentive associated with acquiring domain names either similar to or identical with the names of popular brands is acting as a catalyst for surge in trademark violations on the Internet.

The global reach of Internet is another factor that lends unique character to this revolutionary technological innovation. While distance doesn’t matter in transacting via
cyberspace, it is the transgression of legal rights of an individual that poses challenge for the court to secure physical presence of the party located outside the territorial jurisdiction of the respective court, and enforce its orders.

Broadly, the issues involved in trademark violations on the Internet can be categorised as – Substantive Issues (Domain Name Issues and Techno-Legal Issues) and Procedural Issues ( Jurisdiction).

(1) Domain Name Issues

During the formative years of Internet, domain names were considered as equivalent to real world physical addresses. However, with cyberspace assuming the role of quintessential e-commerce platform, the concept of domain names also underwent dramatic re-configuration. From mere addresses, domain names graduated to online brands that are associated with the goodwill of the owner of domain names. Thus, started the race for claiming online brand identity since domain name registration is based on first-come-first-served rule, which could preclude the owner of trademark from claiming first right on the identical domain name. The opportunistic domain name registrants saw a goldmine in well-known names and registered identical and / or similar domain names in bulk so that when the trademark owners seek to register domain names of their choice, they were served with ‘Not Available’ message. The original registrants of such domain names, now, come into picture and offer to sell the domain names desired by the trademark owners at a price much higher than the registration cost of such domain names. Such a scenario is not an isolated case pertaining to abuse of domain name registration process. The issues that germinate on account of domain name abuse, and resultant trademark violations in cyberspace, include:

(i) Cybersquatting: U.S. legislation, Anti-Cybersquatting Consumer Protection Act (ACPA), 1999, defines a cybersquatter as anyone who, with bad faith intent to profit, (a) registers, (b) traffics in, or (c) uses a domain name, that is identical with or confusingly similar to a distinctive mark or dilutive of a famous mark. However, the ACPA is also criticised for being over-protective of celebrity names and well-known marks. The term ‘cybersquatter’, generally, refers to a legal person lacking a legitimate claim over the domain name, but still registers it for any of the following purposes: (a) to sell the same for profit, or (b) to prevent the trademark holder from gaining access to the name, or (c) to divert traffic to another website, or (d) to harass or ridicule the competitor or prevent them from establishing a website using that name. NSI’s (later,
ICANN’s) omission to investigate the prior existence of trademarks in relation to requested
domain names has resulted in the registration of domain names, comprising several well-known
corporate and personal names, by third parties to which they have no legitimate right. The most
glaring examples of cybersquatting involved a Swiss businessman who had registered
www.schweiz.ch, www.suisse.ch and www.svizzera.ch (‘Switzerland’ in German, French and
Italian) in 1995 and directed the users to a website that offered an e-mail service and sold Swiss-themed
accessories marked with Switzerland’s red and white flag. However, the matter was finally resolved in
2006 when WIPO transferred the right of using the infringing domains to the Swiss government.\(^1\) The
menace of cybersquatting not only eats into the goodwill of trademark holders, sometimes, it is
also a silent assassin in that it may take a considerable time before the original trademark holder
becomes aware of the cybersquatting problem.

(ii) **Typosquatting:** Cybersquatting may take the form of typosquatting, where the domain name
registrant registers a variant of a famous trademark. For instance, micros0ft.com (for
microsoft.com), siffy.com (for sify.com), yaho.com (for yahoo.com), etc. The purpose
of a typosquatter is the same as that of a cybersquatter; only the mode of trademark infringement is
slightly different.

(iii) **Domain Name Parking:** Domain name parking occurs when a domain name registrant
deposits its domain names with a Registrar or Parking Service Provider who “creates placeholder
pages and then invites...Internet advertisement networks to fill them with advertisements” as
opposed to constructing a functional website.\(^2\) Domain Parking generates money when the user
click on links to other websites advertised on the parked page and for every such click; the
advertiser indirectly pays the domain name registrant. This kind of activity is commonly referred
to as Pay-Per-Click (PPC) advertising. Domain name parking results in trademark infringement
because unaffiliated domain name registrants can incorporate the owners’ marks into parked

---

\(^1\) *Beware Cybersquatters And Typosquatters*, 20 (5) Ancestry Magazine (September/October 2002),

F01 (relaying a law professor’s assertion that “the practice amounts to someone making money off
someone else’s trademark without permission.”). Additionally, when Internet users arrive at the parked
sites and click on the advertisements, the Internet advertisement networks receive payment from the
advertisers and pass on a portion of the revenue to the domain name registrant.
domain names; thereby, reducing the trademark owner’s ability to control the use of their mark in cyberspace and diverting consumers to competitors’ websites.³

(iv) **Gripe / Protest Websites:** Gripe / Protest websites are a tool to register protests against any alleged shortcoming of the original website or against a brand name, in general. Typically, the domain names of such websites are formed by suffixing words, like ‘sucks’, ‘I hate’, and other similar phrases, to the name of the original website. For example, www.microsftsucks.com could be a gripe / protest website of www.microsoft.com. Similarly, ihateyahoo.com could be a gripe / protest website for yahoo.com.

(v) **Reverse Domain Name Hijacking:** Harte defines Reverse Domain Name Hijacking as a scenario when “large corporations use their legal and financial muscle to evict legitimate domain name holders from valuable registrations that they want.”⁴ Further, ICANN’s Domain Name Uniform Dispute Resolution Policy (UDRP) defines Reverse Domain Name Hijacking as using the UDRP in bad faith to attempt to deprive a registered domain name holder of a domain name.⁵

(vi) **Domain Tasting:** The domain name registrants are usually given a five-day grace period between the time a domain name is registered and the payment for owning the domain is due. The idea was floated to enable registrants to fix mistakes, like accidentally misspelling a new domain name. This golden window of opportunity, however, led to the rise of a trend, known as “domain tasting” whereby, computer users sample large numbers of domain names, placing advertisements on the otherwise empty website, and testing to see how much advertisement revenue each name can generate.

(vii) **Domain Kiting:** Domain Kiting is the corollary of Domain Tasting with registrants cancelling their domain name just before the grace period expires, and followed by their immediately re-registering it. By repeating this process *ad infinitum*, payment for the domain is postponed indefinitely and yet the registrant at the same time is making money with the domain name.

---


⁵ Rules for Uniform Domain Name Dispute Resolution Policy, Rule 1.
Current Legal Position of Domain Name Issues: The courts in U.S.A. apply relevant provisions of Lanham Act, 1946, Federal Trademark Dilution Act (FTDA), 1995, and Anti-Cybersquatting Consumer Protection Act (ACPA), 1999, in order to resolve different domain name issues. Lanham Act, 1946 is a Federal Trademark legislation, which inter alia prohibits a number of activities, including trademark infringement, trademark dilution, and false advertising. Lanham Act defines the term “trademark” as “word, name, symbol, or device, or any combination thereof used by a maker or seller of goods to identify and distinguish their goods from those made or sold by others. The Lanham Act offers a trademark owner three major causes of action to protect their trademark rights: (a) trademark infringement, (b) unfair competition, and (c) dilution. The FTDA defines dilution as lessening of the capacity of a famous mark to identify and distinguish goods or services, regardless of the presence or absence of (a) competition between the owner of the famous mark and the other parties, or (b) likelihood of confusion, mistake or deception. The FTDA lists eight factors that determine if a mark is famous for purposes of the Act:

A. the degree of inherent or acquired distinctiveness of the mark;
B. the duration and extent of use of the mark in connection with the goods or services with which the mark is used;
C. the duration and extent of advertising and publicity of the mark;
D. the geographical extent of the trading area in which the mark is used;
E. the channels of trade for the goods or services with which the mark is used;
F. the degree of recognition of the mark in the trading areas and channels of trade used by the marks’ owner and the person against whom the injunction is sought;
G. the nature and extent of use of the same or similar marks by third parties; and
H. whether the mark was registered.

FTDA does not specifically prohibit cybersquatting. If the cybersquatter does not attempt to sell trademark based domain names to the rightful trademark owner, but rather

---

9 S. REP. NO. 106-140, at 7 (1999)
sits on it to curtail the trademark owner’s use, it seems that the cybersquatter can avoid commercial use, and escape liability under dilution.\textsuperscript{10}

ACPA specifically defines a cybersquatter as anyone who registers, with bad faith, a domain name that is identical with or confusingly similar to a distinctive mark or dilutive of a famous mark. The ACPA lays down a non-exhaustive list of nine factors that court may consider in determining whether there is bad faith, including, among others, (a) the trademark or other intellectual property rights of the person, if any, in the domain name; (b) the extent to which the domain name consists of the legal name of the person or a name that is otherwise commonly used to identify that person; (c) the person’s prior use, if any, of the domain name in connection with the \textit{bona fide} offering of any goods or services; (d) the person’s \textit{bona fide} non-commercial or fair use of the mark in a site accessible under the domain name; (e) the person’s intent to divert consumers from the mark owner’s online location to a site accessible under the domain name that could harm the goodwill represented by the mark, either for commercial gain or with the intent to tarnish or disparage the mark, by creating a likelihood of confusion as to the source, sponsorship, affiliation, or endorsement of the site; (f) the person’s offer to transfer, sell, or otherwise assign the domain name to the mark owner or any third party for financial gain without having used, or having an intent to use, the domain name in the \textit{bona fide} offering of any goods or services, or the person’s prior conduct indicating a pattern of such conduct; (g) the person’s provision of material and misleading false contact information when applying for the registration of the domain name, the person’s intentional failure to maintain accurate contact information, or the person’s prior conduct indicating a pattern of such conduct; (h) the person’s registration or acquisition of multiple domain names which the person knows are identical or confusingly similar to marks of others that are distinctive at the time of registration of such domain names, or dilutive of famous marks of others that are famous at the time of registration of such domain names.

names, without regard to the goods or services of the parties; and (i) the extent to which the mark incorporated in the person’s domain name registration is or is not distinctive and famous.\textsuperscript{11}

The courts in the U.S. seem to be divided in their interpretation of available legislations as applicable in domain name issues. In \textit{Intermatic, Inc., v. Denis Toeppen},\textsuperscript{12} where the defendant, an infamous cybersquatter, registered 200 domain names, intending to sell these names to the companies that owned the trademarks, the Illinois court granted an injunction to the plaintiffs preventing the defendant from using the domain name intermatic.com. The court observed that Intermatic’s name and reputation would be at defendant’s mercy and could be linked with any messages on defendant’s website if the domain name were allowed to remain in Toeppen’s control. However, in \textit{Denver Area Education Telecommunications Consortium, Inc. v. Federal Communications Commission},\textsuperscript{13} the U.S. Supreme Court stated that it is not practical to protect domain names since technology is advancing so quickly. The court further noted that it is possible, in the future, that domain names may be considered a form of protected speech. In a recent case of \textit{Warren Weitzman v. Lead Networks Domains Pvt. Ltd.},\textsuperscript{14} the court ruled that a domain name registrant hold acquired Common Law trademark rights by simple ownership and usage in domain names he owned, even though they corresponded to well-known trademarked brand names. Plaintiff, who had parked some 12,000 domain names, filed suit against defendants (Registrar of Domain Names), Lead Networks, located in India, over 22 domain names, 21 of which were .com TLDs. He filed the case in Virginia, claimed \textit{in rem} jurisdiction against .com registry and the .org registry under the ACPA, claiming that the domain names were “extremely valuable earning in excess of USD 2,000 a month from parking and were worth in excess of USD 2,000,000.” He further alleged that the Registrar had “taken control of his domains” and was, in fact, parking the domain names themselves. The court, upon not receiving an answer from the defendant Registrar, ordered the transfer of domain names back to the domain holder. The surprising part of this case was the fact that some of the domain names at issue were typos of famous trademarks, like pirrelli.com, reabok.com, oncologics.com, etc.

In the U.K., domain name disputes are resolved by resorting to relevant provisions of Trade Marks Act (TMA), 1994, and the Common Law remedies available under the tort of

\textsuperscript{11} 15 U.S.C. Section 1125(d)(1)(B)(i)
\textsuperscript{12} 947 F. Supp. 1227, 1996 US Dist.
\textsuperscript{13} 518 U.S. 727 (1996)
\textsuperscript{14} Case No. 1:2009cv01141 (US Dist. E.D.V)
passing-off and conspiracy. Section 10(1) of TMA states that trademark infringement occurs if a person uses in the course of trade a sign that is identical with the trademark in relation to goods or services, which are identical with those for which it is registered. Thus, the concept of ‘likelihood of confusion’ is not incorporated under Section 10(1), TMA. However, the domain name disputes can still be addressed under this section on the yardstick of following questions:

(A) Whether the domain name in question is identical to the registered trademark?\(^\text{15}\)

(B) Whether the use of domain name is in the course of trade?

(C) Whether such use is in relation to identical goods or services for which the trademark is registered?

The tort of passing-off was conceived by the U.K. courts in order to protect all those marks that are not registered under the Statute. It follows that if a person claiming to use and own a domain name but does not have a registered trademark; he may turn to the Common Law tort of passing-off. For a claim of alleged passing-off to succeed, Lord Oliver in *Reckitt & Colman Products Ltd v Borden Inc.*\(^\text{16}\) laid down the “classic trinity” test thus:

“The law of passing-off…may be expressed in terms of the elements, which the plaintiff in such an action has to prove in order to succeed…First, he must establish a *goodwill or reputation attached to the goods or services*, which he supplies, in the mind of the purchasing public by association with the identifying get-up…under which his particular goods or services are offered to the public, such that the get-up is recognised by the public as distinctive specifically of the plaintiff’s goods or services. Secondly, he must demonstrate a *misrepresentation by the defendant to the public* (whether or not intentional) leading or likely to lead the public to believe that goods or services offered by him are the goods or services of the plaintiff…Thirdly, he must demonstrate that he suffers or, in a *quia timet*\(^\text{17}\) action, that *he is likely to suffer damage* by reason of the erroneous belief engendered by the defendant’s misrepresentation…” (emphasis added)

The courts in U.K. also adopt non-uniform interpretation of available legislative and non-legislative remedies in domain name disputes. While in *Harrods Limited v. UK Network*

\(^{15}\) However, ‘identical’ does not amount to absolutely identical.

\(^{16}\) [1990] RPC 341

\(^{17}\) An injunction to restrain wrongful acts, which are threatened or imminent but have not yet been commenced.
the defendants, registrants of harrods.com, were held liable at interlocutory level for passing-off and trademark infringement. Harrods, the famous luxury department store, argued that the ‘Harrods’ trademark was a well-known mark, which would suffer damage to its goodwill or dilution if used by the competitor in a domain name, to which they had no lawful connection or legitimate interest. However, later in *Avnet v. Isoact*, the court held that since the services provided by the defendants were quite different from those of the plaintiffs, there was no infringement of the trademark under Section 10(1), TMA, if the word ‘Avnet’ is used in the disputed domain name.

(2) Techno-Legal Issues

Trademark trafficking in cyberspace through domain names involves registration of the infringing domain names with a Registrar. However, there are certain other issues that contribute to the problem, but pose more techno-legal issues than purely legal interpretation. Since Internet is a modern technology that keeps on improving by the minute, encroachment of legal field by technology, at times is inevitable. The techno-legal issues that contribute to trademark trafficking on the Internet include:

(i) **Meta tags**: Meta tags are terms, written in HTML within a web page, that describe the contents of that page. The more often a search term appears within a website’s Meta tags and text, the more likelihood of a Search Engine placing that web page at the top of its list of search results. When one of the keywords in a website’s Meta tags is a trademark owned by a competitor, controversy exists as to whether or not this constitutes trademark infringement or dilution. On the one hand, mere presence of a competitor’s trademark in the Meta tags is arguably evidence of trying to piggy-back off the goodwill of a company by drawing their customers away from their intended target, and towards the Meta tag owner’s site instead. And on the other hand, obtaining an advantageous marketing position is not necessarily prohibited by trademark law.

(ii) **Hyperlinks**: A link allows the users of Internet to navigate to (a) specific part of material within the same web page; (b) specific web page within the same website; or (c) another website (or to specific web page within another website). A link can be placed within the simple text.

---

18 unreported HC, Chancery Division, 9 December 1996
20 Text containing links is called Hypertext.
such that when the computer mouse pointer is run over that text, the pointer is turned into a small hand-like image that suggests the presence of a HREF link on that text. The location to which the link directs can be visited by simply clicking on that link. Similarly, a link can also be embedded within a graphical image or button or any other object. It is the linking ability that makes the Internet robust and convenient for even a non-technical individual to browse. A link that leads an end user to falsely believe that a web page is affiliated or approved by the target web page could be a trademark infringement. For example, an image link that puts another’s trademark on the source web page to create the impression of an endorsement.

(iii) **Frames:** Frame is essentially an HTML tag that allows the user to keep the top portion of the page stationary and when the user clicks on a link it will load another page in the window below or next to it. With frames, the user can display more than one HTML document in the same browser window. Each HTML document is called a frame, and each frame is independent of the others.\(^{21}\) A web page that includes framing will consist of specifically identified areas, i.e. ‘frames’, on the computer page. Framing technology allows the framing website - with its logo and third-party advertising conspicuously displayed - to remain as the frame or border of the framed site. Moreover, when frames are used, the URL does not change; it continues to display the address of the framing site rather than that of the framed page. This URL discrepancy may confuse casual browsers who are not sure if they have left the initial site or are viewing material created by another site owner.\(^{22}\)

(iv) **Search Engine Advertising:** Search Engine Advertising refers to the practice of using the Search Engine for advertising purposes via multiple means, including selling keywords to the highest bidder in return for ensuring higher placement in the search results, and selling keyword-linked banner advertisements on websites.\(^{23}\) Given the heavy reliance on descriptive terms that Search Engines need in order to properly function, it is inevitable that websites will attempt to employ trademarks, even other company’s trademarks, as part of the descriptive shorthand of

---


Internet navigation. Whether the use of these trademarks constitutes infringement in cyberspace, just like in the real world, is highly dependent on the context.\(^\text{24}\)

(v) **Pop-ups:** A pop-up is a small window that is displayed on top of the existing windows on screen and appears out of nowhere as the user is viewing content on the Web. A pop-up window can be used in any application to display new information. It is widely used on web pages to cause an advertisement to ‘pop up’. Many advertisements display trademarks or lead to other websites that display trademarks. Additionally, trademarks are often incorporated into the programming code that triggers targeted ads to appear.\(^\text{25}\)

(vi) **Mousetrapping:** Mousetrapping is an aggressive marketing technique that forces the users to remain on a specific website, sometimes while disabling their browser functions or flooding them with pop-up advertisements. Whenever the user tries to leave the site by using the ‘back’, ‘forward’ or ‘close’ buttons, a new window is automatically opened that prevents the browser from leaving the site. To exit the loop, the user is forced to end the task or reboot his computer.\(^\text{26}\) At least one case has been reported from the U.S. involving trademark infringement by Mousetrapping technique.

(vii) **Spam:** Unsolicited commercial or non-commercial emails or messages comprising trademark-infringing content also pose a techno-legal challenge for the courts.

(viii) **Online Auction Sites:** Immense popularity of online auction websites notwithstanding, they do have to, sometimes, confront the problem of trademark dilution and infringement via the activities of its members, who sell counterfeit and trademark-infringing goods.

**Current Legal Position of Techno-Legal issues:** The courts, in general, have extended protection to the complainants in trademark violations relating to the aforementioned techno-legal issues. However, there is still lack of clarity among the judges while deciding disputes concerning techno-legal issues.\(^\text{27}\)


\(^{27}\) See, for example, Reed Executive Plc. v Reed Business Information Ltd. [2004] EWCA Civ. 159, where the court observed “…as for Meta tags, it could not be said that there was infringement since, even
(3) Jurisdiction

Jurisdiction refers to the authority (of a body-political or otherwise) for interpretation and application of laws and administration of justice. More specifically, jurisdiction is the authority of a court to hear a case and resolve a dispute involving person, property, and subject matter. All sovereign independent States possess jurisdiction over all persons and things within its territorial limits and all causes, civil and criminal, arising within these limits.

Internet poses some of the toughest jurisdictional questions because of its inherent global nature. If A, a resident of Pakistan, commits a trademark infringement in cyberspace against a website owned and operated by B, an Indian resident, how can courts in India ensure enforcement of their decision considering the acrimonious relations between the two sovereign nations?

In U.S.A., the State courts assert personal jurisdiction over entities located outside of the State using “long-arm Statutes.” Long-arm statutes differ from State to State, but tend to be similar. The doctrine of “long-arm Statute” authorises the courts to claim personal jurisdiction over a non-resident defendant whose principal business is outside the State on the ground that their action (tortuous or otherwise) falls within the nature of activity required to qualify for jurisdiction. The name “long-arm” comes from the purpose of these statutes, which is to reach into another State and exercise jurisdiction over a non-resident defendant.

Similarly, there is a provision for in rem proceedings against the defendant under Anti-Cybersquatting Consumer Protection Act, 1999. To cover situations in which the mark owner cannot bring a cause of action against a potential defendant because such defendant is not subject to in personam jurisdiction, or has successfully eluded the plaintiff, the ACPA permits the mark owner to file suit literally against the domain name itself. In order to proceed with this in rem action against the domain name, the mark owner must send a notification of intent to proceed in rem to the postal and e-mail addresses given by the domain name registrant to the Registrar and by publishing notice of the action as the court may direct after filing. The res is deemed to be

if the employment of a Meta tag fell within the scope of an infringing act, being a ‘trademark use’, there would still be no confusion. As to ‘use’, it would be strange if the use of a trademark as a Meta tag were sufficient use to enable that mark to withstand a revocation challenge on the basis of non-use if that were the sole use made of the mark.

28 Study Material of Asian School of Cyber Laws’ Online Course “Diploma in Information Technology (DITL)”, Jurisdictional Issues, at 305.
located in the Federal judicial district in which the authority that registered or assigned the domain name is located, and the action may be brought in that Federal judicial district.

The long-arm Statutes and *in rem* jurisdiction can work effectively within a country. However, when the parties are located in different countries, the effectiveness of these provisions in the Statutes, in the absence of international cooperation or binding treaties and conventions, remains doubtful.

The courts in U.S.A. are a divided house when it comes to determining jurisdiction over a defendant accused of trademark trafficking in cyberspace. However, the most reliable judgment till date came has been *Zippo Manufacturing Company v. Zippo Dot Com, Inc.*, 30 where the court proposed a Sliding Scale analysis to determine jurisdiction in trademark violation cases on the Internet. The court proposed that personal jurisdiction should be exercised in proportion to the quality and nature of commercial activity exercised over the Internet. The court noted that the cases in this genre reveal a ‘sliding scale’, in which, “...at one end of the spectrum are situations where a defendant clearly does business over the Internet. If the defendant enters into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the Internet, personal jurisdiction is proper. At the opposite end are situations where a defendant has simply posted information on an Internet website, which is accessible to users in foreign jurisdictions. A passive website that does little more than make information available to those who are interested in it is not grounds for the exercise of personal jurisdiction. The middle ground is occupied by interactive websites where a user can exchange information with the host computer. In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and [the] commercial nature of the exchange of information that occurs on the website.”

**4) Trademark Trafficking in Cyberspace: The Indian Context**

The courts in India rely on Trade Marks Act, 1999, and the Common Law remedy available under the tort of passing-off while deciding disputes pertaining to trademark trafficking in cyberspace. The jurisdictional powers are derived from Section 20, Code of Civil Procedure, 1908, which provides that the suit is to be instituted in the court:

(a) within the local limits of whose jurisdiction the defendant (or one of them) at the time of the commencement of the suit actually or voluntarily resides or carries on business or personally works for gain; or
(b) within the local limits of whose jurisdiction the cause of action, either wholly or in part, arises.

By implication, a court in India would have jurisdiction to entertain a domain name dispute, even if the defendant resides outside the country, in case the plaintiff establishes that the cause of action arose within the territorial jurisdiction of the court.

The development of law relating to trademark trafficking in cyberspace in India is still in its nascent stages. However, Indian courts have, to a large extent, inclined in favour of complainants and protected the online brand identity of the famous names.

Starting with *YAHOO! Inc. v. Akash Arora & Anr.* 31 in 1999, which was decided by Delhi High Court, the trademark disputes in cyberspace have reached Indian courts with consistent regularity. However, the Supreme Court of India had a rare chance to adjudicate upon the issue in *Satyam Infoway Ltd. v. Sifynet Solutions (P) Ltd.* 32 where the Apex Court reiterated the observations of several High Courts to the effect that “the use of the same or similar domain name may lead to a diversion of users, which would result from such users mistakenly accessing one domain name instead of another. This may occur in e-commerce with its rapid progress and instant (and theoretically, limitless) accessibility to users and potential customers and particularly so, in areas of specific overlap. Ordinary consumers/users seeking to locate the functions available under one domain name may be confused if they accidentally arrived at a different but similar website, which offers no such services. Such users could well conclude that the first domain name owner has misrepresented its goods or services through its promotional activities, and the first domain owner would thereby lose its customers. It is apparent, therefore, that a domain name may have all the characteristics of a trademark and could found an action for passing-off.”

The issue of jurisdiction in domain name disputes was discussed threadbare by the Delhi High Court in *Banyan Tree Holding (P) Ltd. v. A. Murali Krishna Reddy.* 33 The court laid

---

31 1999 PTC (19) 201 (Del)
32 (2004) 6 SCC 145
33 Suit No.: CS (OS) No.894/2008. Date of Decision: November 23, 2009
down the following settled legal position as far as jurisdiction of Indian courts in domain name disputes is concerned:
(i) Mere accessibility of the defendants’ website in a jurisdictional territory would not enable a court to exercise jurisdiction;
(ii) A passive website, with no intention to specifically target audiences outside the State where the host of the website is located, cannot vest the Forum Court with jurisdiction;
(iii) For the purposes of a passing-off action or an action for infringement where the plaintiff is not carrying on business within the jurisdiction of the Forum Court, and where there is no long-arm Statute, the plaintiff would have to show that the defendant purposefully availed itself of the jurisdiction of the Forum Court;
(iv) It is not enough merely to show that the website hosted by the defendant is an interactive one. It would have to be shown that the nature of the activity indulged in by the defendant by the use of the website was with an intention to conclude a commercial transaction with the website user;
(v) The issue of incorporating filters to block access to the website by viewers located outside the Forum State will have to be considered while deciding if the defendant had “purposefully avoided” the Forum State. However, that question will arise only if the plaintiff has been able to show that the website of the defendant is interactive and permits commercial transactions to be concluded by the defendant with a user of the website;
(vi) Jurisdiction of the Forum Court does not get attracted merely on the basis of interactivity of the website, which is accessible in the Forum State. The degree of interactivity apart, the nature of the activity permissible and whether it results in a commercial transaction has to be examined;
(vii) For the “Effects” test to apply, the plaintiff must necessarily plead and show prima facie that the specific targeting of the Forum State by the defendant resulted in an injury or harm to the plaintiff within the Forum State;
(viii) For the purposes of a passing-off or an infringement action (where the plaintiff is not located within the jurisdiction of the court), the injurious effect on the plaintiff’s business, goodwill or reputation within the Forum State as a result of the defendant’s website being accessed in the Forum State would have to be shown. This would require the presence of the plaintiff in the Forum State and not merely the possibility of such presence in the future;
(ix) To show that an injurious effect has been felt by the plaintiff, it would have to be shown that viewers in the Forum State were specifically targeted. Therefore, the “Effects” test would have to be applied in conjunction with the “Sliding Scale” test to determine if the Forum Court has jurisdiction to try a suit concerning Internet based disputes;

(x) The commercial transaction entered into by the defendant with an Internet user located within the jurisdiction of the Forum Court cannot possibly be a solitary trap transaction since that would not be an instance of “purposeful availment” by the defendant. It would have to be a real commercial transaction that the defendant has with someone not set up by the plaintiff itself. If the only evidence is in the form of a series of trap transactions, they have to be shown as having been obtained using fair means. The plaintiff seeking to establish jurisdiction on the basis of such trap transactions would have to aver unambiguously in the plaint, and also place along with it supporting material, to prima facie show that the trap transactions relied upon satisfy the above test.

(5) Alternative Dispute Redressal (ADR) Mechanism

In its efforts to provide an administrative-level solution to the domain name disputes, ICANN has formulated Uniform Domain-Name Dispute Resolution Policy (UDRP), which allows trademark and service mark holders to arbitrate certain claims against a domain name registrant before an Approved Dispute Resolution Service Provider. Rules for Uniform Domain Name Dispute Resolution Policy (the “Rules”) supplement the policy and lay down the procedure to be adopted during administrative proceedings for the resolution of disputes under the ICANN UDRP. Additionally, such proceedings are also governed by the Supplemental Rules of the Provider administering the proceedings, as posted on its website. To the extent that the Supplemental Rules of any Provider conflict with these Rules, these Rules supersede.

There are currently four ICANN-Approved Dispute Resolution Providers:

(i) Asian Domain Name Dispute Resolution Centre (ADNDRC)
(ii) National Arbitration Forum (NAF or FORUM)
(iii) World Intellectual Property Organisation (WIPO)
(iv) Arbitration Centre for Internet Disputes (Czech Arbitration Court or CAC)

The domain name disputants are free to choose the forum where they want to litigate. However, over the years, the disputants have demonstrated their preference of WIPO over other forums to adjudicate upon the dispute.
For a complaint to succeed under UDRP, the complainant must demonstrate that a respondent has violated all three of the following elements:

(i) The domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights;

(ii) The respondent has no legitimate interests to the domain name; and

(iii) The respondent has registered and is using the domain name in bad faith.  

In order to succeed in a UDRP proceeding, the complainant must prove respondent’s bad faith in domain name registration, which can be evidenced by proving any of the following circumstances:

(i) indicating circumstances that show that the registration is done primarily for the purpose of selling, renting, or otherwise transferring the domain name registration to the complainant who is the owner of the trademark or service mark; or to a competitor of that complainant, for valuable consideration in excess of the documented out-of-pocket costs directly related to the domain name; or

(ii) the domain name is registered in order to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name, provided that the registrant has engaged in a pattern of such conduct; or

(iii) the domain name is registered primarily for the purpose of disrupting the business of a competitor; or

(iv) by using the domain name, the registrant has intentionally attempted to attract, for commercial gain, Internet users to registrant’s website or other online location, by creating a likelihood of confusion with the complainant’s mark as to the source, sponsorship, affiliation, or endorsement of registrant’s website or location or of a product or service on registrant’s website or location.  

However, the respondent can negate a bad faith plea of the complainant by proving any of the following:

(i) use of, or demonstrable preparations to use, the domain name or a name corresponding to the domain name in connection with a bona fide offering of goods or services, before any notice of the dispute was received; or

34 Paragraph 4(a), UDRP
35 Paragraph 4(b), UDRP
(ii) the respondent was commonly known by the domain name, even if they had not acquired trademark rights; or
(iii) the respondent is making a legitimate non-commercial or fair use of the domain name, without intent for: commercial gain, or misleadingly diverting consumers, or to tarnishing the trademark at issue.\textsuperscript{36}

The Arbitration Panel of experts can give any of the following decisions pursuant to the conclusion of arbitration proceedings:
(a) Cancellation of domain name registration; or
(b) Transfer of domain name registration; or
(c) Decide in favour of the domain name registrant (i.e., deny the requested remedy). In this regard, if the Panel concludes that the dispute is not within the scope of Paragraph 4(a) of the UDRP, it must specify this in its decision. Also, if after considering the submissions of the parties, the Panel finds that the complaint was brought in bad faith, the Panel is required to declare in its decision that the complaint was brought in bad faith and constitutes an abuse of the administrative proceeding.\textsuperscript{37}

WIPO has been in the forefront of fight against domain name offenders in cyberspace. Till date, UDRP proceedings administered by the WIPO Centre have involved parties from 161 countries across the world.\textsuperscript{38} The parties can draw upon a growing list of over 1,000 independent WIPO arbitrators, mediators and experts from some 70 countries.\textsuperscript{39} Since commencing its domain name dispute resolution service in December 1999, the WIPO Centre has processed 19,569 cases,\textsuperscript{40} involving 35,481 domain names,\textsuperscript{41} of which 18,998 cases have been resolved.\textsuperscript{42}

In India, .in ccTLD registration is managed by INRegistry, which was created by NIXI, a Government of India undertaking. As part of registration, the registrants are required to submit to a mandatory arbitration proceeding under the .IN Domain Name Dispute Resolution Policy

\textsuperscript{36} Paragraph 4(c), UDRP
\textsuperscript{37} Paragraph 3, UDRP
(INDRP), which is supplemented by the INDRP Rules of Procedure. INDRP is similar to ICANN UDRP and the Arbitration Panel comprises of experts who have proven expertise in the subject.

Internet has been around for decades, but its pervasiveness has been felt the most during the first decade of Twenty First Century. Resultantly, cyberspace has spawned many a legal issues that have yet to be resolved in a satisfactory manner by the courts across different jurisdictions.

Trademark trafficking in cyberspace has been rampant thanks to the sustained efforts of the traffickers to get maximum pecuniary benefit from the lack of policing on the Internet. However, certain legal and administrative measures have slowed down the terror unleashed by trademark violators in cyberspace. The need of the hour is to adopt a balancing approach, which tackles the issue with the help of both technology and law.

Some tough decisions at the national and international level are required to address the issue. Current impossibility of the measures should not mean cessation of efforts to achieve international consensus among the sovereign nations. Legislative, judicial, and administrative machineries – both at national and international levels – need to work in tandem to thwart the designs of Pirates of Cyberia.