CHAPTER-VII
CONCLUSION AND SUGGESTIONS

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 everincreasing 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).

**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 ecommerce 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 overprotective 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. 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, microsOft.com (for microsoft.com), siffy.com (for sify.com), yaho.com (for yahoo.com), etc. The purpose of a typo squatter 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. 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 domain names; thereby, reducing the trademark owner's ability to control the use of their mark in cyberspace and diverting consumers to competitors' websites.

(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.microsoftsucks.com could be a gripe I protest website of www.microsoft.com. Similarly, ihateyahoo.com could be a gripe I 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." 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.

---

2 Leslie Walker & Brian Krebs, The Web's Million-Dollar Typos, Washington Post, April 30, 2006, at FOI (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


4 Ada A. Harte, The Domain Name Debate, (2001) 2 (1) TELJ 2, at 5

5 Rules for Uniform Domain Name Dispute Resolution Policy, Rule 1
(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.

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 sits on it to curtail the trademark owner's use, it seems that the cybersquatter can avoid commercial use, and escape liability under dilution.

ACP A 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 ACP A 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

---

9 S. REP. NO. 106-140, at 7 (1999)
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 bonafide offering of any goods or services; (d) the person's bonafide 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 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, 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.11

The courts in the U.S. seem to be divided in their interpretation of available legislations as applicable in domain name issues. In Intermatic, Inc., v. Denis Toeppen,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 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 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 in rem jurisdiction against .com registry and the .org registry under the ACP A, 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 pirreli.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

\textsuperscript{13} 518 U.S. 727 (1996)
\textsuperscript{14} Case No. 1:2009cv01141 (US Dist. E.D.V)
available under the tort of 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 plaintiffs 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

\(^{15}\) However, 'identical' does not amount to absolutely identical

\(^{16}\) [1990] RPC 341
must demonstrate that he suffers or, in a quia timet\textsuperscript{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 Services Limited & Others,\textsuperscript{18} 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,\textsuperscript{19} 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 'A vnet' is used in the disputed domain name.

**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

\textsuperscript{17} An injunction to restrain wrongful acts, which are threatened or imminent but have not yet been commenced

\textsuperscript{18} unreported HC, Chancery Division, 9 December 1996

\textsuperscript{19} [1998] F.S.R. 16

404
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\textsuperscript{20} 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.\textsuperscript{21} A web page that includes framing will consist of specifically identified areas, i.e. 'frames', on the computer page. Framing

\textsuperscript{20} Text containing links is called Hypertext
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.  

(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.  

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.

(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

---


23 Mylene Mangalindan, Playing The Search-Engine Game, THE WALL STREET JOURNAL, June 16, 2003, available at http://www.morevisibility.com/newfws\playin\--the_searchengine-\-game.html. Last accessed on October 30, 2016. These banners allow a site owner to pay for a graphical banner advertisement, or pop-up advertisement, delivered to a Web user after the user searches for selected keywords

24 David M. Fritch, Searching For Initial Interest Confusion And Trademark Protection In Cyberspace, 6 PGH. J. Tech. L. & Pol'y 1, at 121
other websites that display trademarks. Additionally, trademarks are often incorporated into the programming code that triggers targeted ads to appear.\textsuperscript{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.\textsuperscript{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.\textsuperscript{27}


\textsuperscript{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 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
**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 AntiCybersquatting 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 ACP A 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-

---

28 Study Material of Asian School of Cyber Laws' Online Course "Diploma in Information Technology (DITL)", Jurisdictional Issues, at 305
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 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.,\textsuperscript{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

\textsuperscript{30}952 F. Supp. 1119 (E.D. Penn., Jan. 16, 1997)
of interactivity and [the] commercial nature of the exchange of information that occurs on the website.”

**Trademark Trafficking in Cyberspace: Position in India**

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, anses.

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."

---

\(^ {31} \) 1999 PTC (19) 201 (Del)
\(^ {32} \) (2004) 6 SCC 145
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. The court laid 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 longarm 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;

33 Suit No.: CS (OS) No.894/2008. Date of Decision: November 23, 2016
(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.

**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.\(^{34}\)

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.\(^{35}\)

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

\(^{34}\) Paragraph 4(a), UDRP

\(^{35}\) Paragraph 4(b), UDRP
(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

(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.\(^\text{36}\)

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.\(^\text{37}\)

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.\(^\text{38}\) The parties can draw upon a growing list of over 1,000 independent WIPO arbitrators, mediators and experts from some 70 countries.\(^\text{39}\) Since commencing its domain name dispute resolution service in December 1999, the WIPO Centre has processed

\(^{36}\) Paragraph 4(c), UDRP
\(^{37}\) Paragraph 3, UDRP
19,569 cases, involving 35,481 domain names, of which 18,998 cases have been resolved.

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 (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.

Suggestions

Admittedly, there is no dedicated legislation in countries, like U.S.A., U.K., and India, in order to deal with different aspects of trademark trafficking in cyberspace. All that the courts in these countries have done is to extend the

---

scope of existing trademark legislation in their respective countries and also, grant Common Law remedy found in the tort of passing-off. "Regretfully, the body of law relating to the Lanham Act has developed into a tangled morass ... Courts struggling to move mountains often find they have only affected minuscule changes in trademark jurisprudence and occasionally have created their own likelihood of confusion. Adding computers to the mix has naturally led to further confusion among judges and litigants.

However, after analysing all the substantive and procedural issues affecting trademark protection in cyberspace, and the national and international response at the legislative, judicial, and administrative level to address such issues, listed in the subsequent paragraphs are the suggestions and recommendations for effective redressal of different trademark issues in cyberspace.

1 Suggestion for Strengthening Legislative and Judicial Framework

1.1 Harmonisation of Jurisdictional Norms

Various judicial approaches and viewpoints are adopted on domestic and national level. Such approaches towards internet jurisdiction are not workable for global protection. Each country having its own legal frame work will not resolve this problem. Hence global solution for such a global problem is recommended. An international instrument specifically dealing with jurisdiction in case of intellectual property rights is the need of the hour. Therefore a specific international treaty in this regard is suggested. The countries of South, East and South-East Asia must enter into a multilateral agreement for general rules of jurisdiction. The rules for determining jurisdiction in physical as well as virtual world must be appropriately addressed.

43 Coach Leatherware Co. v. AnnTaylor, Inc., 933 F.2d 162, 171 (2d Cir. 1991)
44 Kenneth Sutherlin Dueker, Trademark Law Lost In Cyberspace: Trademark Protection For Internet Addresses, 9(2) Harv. 1. L. & Tech. 483 (1996) at pp. 507-508
1.2 Amendments to Trade Marks Act, 1999

The existing trademark law in India should be amended to an extent to accommodate various concurrent uses of trademark over internet. For this the definition of mark can be modified as prescribed in section 2(z) of the Trade Marks Act, 1999. Considering the jurisdictional conflicts prevailing in the cases of trademark infringement and passing off on internet, precise rules on the same should be incorporated in the Act so that Jurisdiction, whether adjudicative or prescriptive, over alleged trademark infringement is not based upon the mere accessibility in a state of a web site containing the allegedly infringing mark.

1.3 Model Code of Private International Law

It is necessary to tailor the international principles of jurisdiction, choice of law and enforcement of judgments making it suitable for dealing with the intellectual property disputes. Hence it is necessary to have a comprehensive conflict of law/private international regime specifically devoted to intellectual property in India. A model code of Private International Law with a specific chapter on Intellectual Property Rights in place will certainly play a significant role in resolving such disputes.

1.4 Comprehensive Legislation on Use of Intellectual property rights in general and trademarks in particular over internet

In order to address the issues relating to intellectual property rights in general and trademarks in particular over internet in form of spamming, cyber-squatting, cyber stalking, hyper-linking, use of trademarks as meta tags, data protection and privacy a comprehensive legislation should be formulated to tighten the legal regime of intellectual property protection in India.
1.5 Enlarged scope of Hague Convention on Choice of Court Agreement, 2005

The Convention excludes consumer and employment contracts and certain specified subject matters (Art. 2). As per article 2, the cases of infringement of intellectual property rights other than copyright and related rights, except where infringement proceedings are brought for breach of a contract between the parties relating to such rights, or could have been brought for breach of that contract are excluded from the scope of this convention. There can only be unification with respect to the intellectual property area if it is included in a treaty on jurisdiction and enforcement that provides for as many nations as possible to participate. The Hague Convention is the ideal tool to unify the rules regarding jurisdiction, recognition, and enforcement in the intellectual property arena. Only the inclusion of all intellectual property rights in the convention including questions of validity will provide certainty in the application and use of this area of law.

1.6 Special Training to Judiciary

Effective enforcement of legislation is always dependent on coherent interpretation of the same. In order to recognize the actual intention of the statutory provisions, professional training should be imparted upon judicial officers. The goal of uniform interpretation can only be achieved when the judicial officers are appropriately skilled and proficient enough to understand the national and international dimensions attached to intellectual property disputes in general and trademark disputes in particular. The periodic training and refresher courses can keep the decision makers abreast of the needs of time and situations and be aware of the important role that they have to play in this developing and ever changing branch of Law.

1.7 Integrated Legislative and Judicial Approach

It is observed that the law has always legged behind the rapid emergence of technological advancement and globalization of trade and
commerce. However, it is near to impossible to keep pace by framing rules on every aspect of technological development and mould the general principles of law accordingly. Territoriality and sovereignty are such concepts which no state can detach from jurisdictional conflicts. The applicability of such legal notions depends much on the efficient, competent and skilful legislative and judicial approach. Therefore, the judiciary as well as the legislature must apply law and frame appropriate laws respectively keeping this in mind.

1.8 Reorientation of National IP Policy

Considering the frequency with which activities involving intellectual property rights cross national borders are taking place, it is utmost important to provide a clear and precise definition of the territorial reach of national intellectual property laws. None of the existing legislations on various types of intellectual property rights in India specifically provides for the territorial delineation. India is in process of drafting National IP policy where this aspect can be incorporated. The National IP Policy specifically provides for enhance protection and enforcement of all types of IPs considering the advancement in the technology. Here the clarity on territorial reach of IP Laws can be addressed. This precision shall help the parties to take appropriate action before an appropriate forum.

2. General suggestion

2.1 Ever since the scope of illegal activity on Internet is discovered, there has been a persistent demand from the legal fraternity to have some kind of international arrangement in the form of a treaty or convention (on the lines of Council of Europe Convention on Cybercrime) under the aegis of UN, which comprehensively covers all aspects of known and potential illegal activities committed on, or with the help of, cyberspace. Further, this treaty should have relevant clauses addressing various jurisdictional issues applicable to all the signatory countries. Any country's access to Internet should be made contingent upon that country's signing and ratification of such a treaty.
However, such drastic measures could be considered draconian by the countries that are opposed to such a treaty.

Admittedly, treaties and conventions are driven by political compulsions and vested interests of the sovereign nations, which make such an idea a utopian one in a highly competitive modern world. Given the nature of prevalent geo-political situation, this is a proposal whose time has not arrived yet.

2.2 Every nation, including India, must strive to draft a comprehensive Cyberspace Code, which inter alia also addresses issues pertaining to Intellectual Property violations in cyberspace.\textsuperscript{45} Trademark trafficking in cyberspace is too technical an issue to be dealt by simply extending the scope of traditional Trademark laws. The collective weight of case law shows that trademark law remains a foundation and serves as a last resort to resolve disputes in cyberspace. Courts, however, need to consider policy implications because the Internet is a new medium of communication that forces trademark law to evolve.\textsuperscript{46} Moreover, the significant differences between trademark registration requirements and domain name registration make the traditional trademark law not a suitable remedy for trademark infringement in cyberspace. Of course, the essence of trademark law should not be lost while drafting specific provisions, rules, and regulations pertaining to trademark violation on the Internet. However, the technical aspects must be given due weight and appropriate treatment while framing the relevant provisions in the Cyberspace Code.

2.3 Another proposal worth exploring is the introduction of a new standardised tag, called \texttt{<trademark>}, which can be added to HTML. This tag would be a non-displaying tag (i.e., any text within the tag would not show up

\textsuperscript{45} Indian Information Technology Act, 2000, strangely, omits to deal with Intellectual Property violations in cyberspace. Even the Information Technology (Amendment) Act, 2008 does not address the issue in any form.

\textsuperscript{46} David Yan, Can We Ride Trademark Law To Surf Cyberspace?, 10 Fordham Intell. Prop., Media & Ent. L. J., 773 (2006) at 861
on the screen to the reader of the website). The `<trademark>` and corresponding `</trademark>` tags could be placed around a list of trademarks held by the owner of the site, which could include company names, product names or slogans. It would be the HTML equivalent of (tm) or (R). As the tag comes into common use, it can be added as a search option to the most popular Search Engines, so that anyone can specifically search for a well-known trademark to find information about that company or its products, whether or not the company has registered its marks as domain names for the site. For example, if Yahoo! website contains the following tag somewhere in the HTML: `<trademark> Yahoo </trademark>`, every Search Engine that reads such a page would store these words as part of the trademark information for the website. Whenever a user wants to find Yahoo's websites, he could search for "<trademark> Yahoo </trademark>," and every one of these pages would show up. However, none of the many third-party websites discussing Yahoo as a company or brand should be found by such a search. Of course, from a technical standpoint, nothing would stop anyone else from adding the `<trademark> Yahoo </trademark>` tag to their website, but such a tag would differ from the use of "Yahoo" in a domain name. By placing the word "Yahoo" in the trademark tag, that site's owner would be stating that it considered "Yahoo" to be its own trademark. That type of claim should fall squarely within the established principles of trademark law, and could be subject to direct challenge by Yahoo. The difference between the `<trademark>` tag and other non-displaying tags, like `<Meta>`, is that `<trademark>` already has a specific legal and business meaning, one which is as relevant to the Web as it is to non-electronic commerce.

2.4 Yan suggests that "harmonising conflicts in cyberspace trademark cases can be resolved through a four-prong inquiry: (i) protecting consumers from the likelihood of confusion; (ii) protecting trademark owners from free riding on goodwill (iii) promoting inter-brand competition; and (iv) preserving public interest. The weight of these factors varies and no one factor is
dispositive. Ultimately, the manner in which these factors are analysed will depend upon the application of the fact-finding tribunal's experience with the mainsprings of human conduct to the totality of the facts of each case. This balancing approach is hereby endorsed and recommended for the judiciary and Arbitration Panels to follow in all trademark disputes in cyberspace.

2.5 Proposals to Address Domain Name Issues

(1) The root cause of domain name issues leading to trademark violations on the Internet is the controversial first-come-first-served policy for domain name registration. This policy was adopted by NSI when Internet took its baby steps towards becoming an institution in itself. It was not anticipated that nondescript domain names, which were not considered more than online addresses or some kind of contact numbers on the Internet, much like the telephone numbers in real world, could be a source of legal problem that still requires proper redressal at multiple levels.

It is recommended that there is a scope for ICANN to keep the application for domain name registration in limbo for a pre-determined time period required for conducting preliminary investigations to determine whether the proposed domain name violates the trademark or service mark rights of any third party. With Search Engines' technology improving at a rapid rate and the ready access to ICANN records, this preliminary investigation should not take more than 710 days to complete.

It is further emphasised that this investigation should be conducted only at a preliminary level, i.e., the investigators should not venture into judicial realm and confine their inquiry into analysing, whether (i) the proposed domain name is virtually the same as an already existing domain name, which is being actively used by its owner; (ii) the proposed domain name is an obvious typo of an already existing domain name; (iii) the

---

47 Id., at 864
48 ICANN currently manages domain name registration
49 The degree of sameness should be that of an average user of imperfect recollection
50 Use should be such as to whether it distinguishes goods and/or services of the domain name holder from the domain name applicant
proposed domain name is an obvious attempt to cybersquat on the domain name, for instance, of a famous celebrity or other well-known mark; (iv) the proposed domain name is used for illegal and/or immoral purposes; (v) the applicant has a record of multiple domain name applications that were either refused at the preliminary investigation stage or at any later stage; and (vi) the applicant is a known collector of potentially infringing domain names.

ICANN may need to augment its resources in terms of recruitment of investigators. Alternatively, this task may be outsourced to another ICANN-approved specialised agency. Further, in order to make the proposal meaningful and effective, this preliminary investigation by ICANN / ICANN-approved agency should be made part of every domain name registration irrespective of the proposed TLD. The proposal may be criticised on the ground that (a) it will make the process of domain name registration time consuming; and (b) legitimate applicants may be denied domain names since the approval will depend on the consent of investigators.

Admittedly, it'll make the process time consuming. However, it is always better to err on the side of caution. As regards the objection on the involvement of human element in domain name registration, such an argument doesn't hold water since even in case of UDRP proceedings, the decision of Arbitration Panellist(s) is(are) enforceable, if not appealed against. In order to make the proposal more effective, some kind of appeal system can also be explored, in case of a negative report from the investigators. In this regard, a negative report should explain the reason(s) for refusal to register the domain name. Such a scrutiny of domain name applications can eliminate the chances of domain name registrations, which prima facie appear fraudulent, dishonest, or in bad faith. It will further help in reducing the number of domain name disputes reaching the courts and/or ICANN-Approved Dispute Resolution Service Providers.

Illegality and immorality should be assessed from the point of view of well-established international legal norms rather than from a specific jurisdictional viewpoint. In this regard, a Statement of Objectives detailing the proposed use of domain name could be sought from the proposer along with the domain name application.
Therefore, ICANN needs to assert itself as an independent body capable of taking decisive measures to arrest the spurt of illegal activities concerning trademark trafficking on the Internet.

(2) The well-known or famous trademarks and celebrity names have often been the target of cybersquatters and typo squatters. However, there is no internationally accepted criterion for determining as to which marks are famous and deserve protection on cyberspace. It is recommended that ICANN undertakes the task of framing an acceptable process that helps in identifying globally famous or well-known marks.

Additionally, domain names comprising names of individuals should, ideally, be given .name or .pro TLD, instead of gTLD .com in order to restrict undesirable uses of domain names in these spaces. This will avoid lots of legal issues concerning trademarks and privacy rights pertaining to the names of celebrities. WIPO, in its Interim Report,\(^52\) states that "some of the strategies employed in these newer domain name spaces included: (a) setting up a "watch" .service to enable people with a legitimate interest in a mark, word, or name corresponding to a domain name to be notified if anyone attempted to register the name, without a requirement that the "watcher" register the name herself; and (b) a "defensive registration" service that allows a person with a legitimate interest in a domain name to register it without having to actively use it." The report also discusses the viability of "exclusion mechanisms" that would prevent the registration of domain names by people likely to utilise them in undesirable ways. However, such exclusion mechanisms have not yet been implemented with respect to any of the new or old gTLDs. In this regard, Lipton suggests maintaining a register of non-permitted uses of specific domain names that would, nevertheless, allow registration and use for other purposes.\(^53\) This might be similar to a restrictive covenant system on a land title registry. For instance, a celebrity, like Julia Roberts, should be entitled to

---


\(^{53}\) Lipton, infra, note 59, at 1420
veto registration of the juliaroberts.com domain name for particular purposes, without: (a) being required to maintain registration of the name herself; and (b) thereby, preventing others from making use of the name in a manner non-objectionable to her.\textsuperscript{54} This "veto" system is, perhaps, a little more sophisticated than alternative approaches suggested by WIPO, because it focuses on allowing the use of a given domain name for specific purposes and only vetoing its use for undesirable purposes.\textsuperscript{55}

Such a "veto" system is recommended for feasibility tests in order to effectively address the abuse of domain name registration process by incorporation of celebrity names in the infringing domain names.

(3) There has been a consistent push for introducing more and more TLDs in order to classify the domain names in certain categories. However, considering the popularity of .com TLD and the initial hype associated with .com, which still retains its charm among domain name aspirants, it is extremely difficult, if not impossible, to confine the domain name registrations to a particular TLD. Moreover, in the absence of a process to filter out applications for different TLDs, anyone can register any domain name with any TLD, provided it is not already taken. The result is that .com is still the preferred TLD for every domain name aspirant. It is recommended that instead of promoting more categories of TLDs, the right approach is to make the system more foolproof with adequate checks and balances that minimize the scope of violations at the entry level, i.e., by introducing the concept of domain name registration application (as discussed in (I) above) instead of the first-come-first-served policy.

(4) ccTLD domain name registration procedure and regional-level domain name registration, like .eu, .asia, etc., allowing for a Sunrise Period to allow trademark owners to apply for registration of domain names to the exclusion of others is a step in the right direction. However, the problem arises once the Sunrise Period expires and the domain name registration is

\textsuperscript{54} Id
\textsuperscript{55} Id at 1421
again reverted to firstcome-first-served basis. The solution lies in discarding this policy and instead, adopting a more reasonable approach of inviting applications for domain name registration (as expounded in (I) above) even at national and regional level.

(5) For legitimate claims to the same domain names, in its Interim Report, WIPO recommended such gateways, which are "a list of names ... with links to distinguish the addresses and their owners from each other." Should Internet users type in www.nielson.com for instance, they are greeted with this message - "Both ACNielsen and Nielson Media Research are linked from this page. However, neither entity holds the 'Nielson' domain as its own." It is unlikely that such gateways will be made compulsory however, as many trademark owners "wish to preserve their unique identity and do not wish to countenance sharing it, even through a portal, with another."

Such a proposal was also endorsed by Jacqueline D. Lipton by observing that "……one potential solution would include entities with competing legitimate interests in a domain name sharing that name by a joint registration and then sharing a home page with hyperlinks to individual websites of the respective interest holders. Technically, this possibility is not particularly problematic. Thus, if a government policy (or private ICANN policy) could be developed to encourage this kind of activity as an alternative to litigation or dispute resolution, society might benefit through greater accessibility to all websites, with similar trademark identities utilising a mutual domain name as a portal to their respective websites. One way of encouraging this kind of activity would be for a government agency or private body authorised by ICANN to specialise in helping those prepared to share a domain name with the technical aspects of setting up the shared main web page with hyperlinks to the respective entities' individual websites. This could be a free service funded, in part, by domain name registration fees, or it could

56 Id, Paragraph 103
57 Id., Paragraph 105
58 Jacqueline D. Lipton, Beyond Cybersquatting: Taking Domain Name Disputes Past Trademark Policy, 40 Wake Forest L. Rev. 1361 (2005)
be a service offered inexpensively by the relevant agency or department as an alternative to more costly litigation or dispute resolution."

Such a proposal is, hereby, endorsed and recommended.

(6) In competing use cases, another possible solution might be to add a brief description of the different businesses in the domain name. For instance, instead of granting domain name like apple.com to any single entity, it makes sense to have descriptive domain names, like applecomputer.com and apple-grocery.com.

(7) Another possible solution to competing use cases could be to add a trademark classification code to each domain name, such as apple.9.com. This will ensure that the treatment of domain names is more in line with regular trademark law. Two parties with the same mark, but operating in dissimilar business areas could both use the mark in their domain names. However, this could mean that the Internet users would no longer be provided with short and easy-to-remember domain names.

(8) Certain administrative measures should be taken to arrest the incidents of Domain Name Parking, Domain Tasting, and Domain Kiting. For instance, domain name registration can be made subject to the setting up of fully functional website on that domain in, say, X number of days, failing which the domain name shall be forfeited. The lesser the number of days, the lesser the chances of abuse of domain name registration process via Domain Parking.

2.6 Proposals to Address Techno-Legal Issues Affecting Trademark Protection in Cyberspace

(1) The techno-legal issues are best addressed with the active help of technology. For instance, several leading Search Engines have modernised and improved their algorithm in order to avoid falling for Meta tags' scam run by trademark traffickers in cyberspace. In recent times, the intense competition among various Search Engines has fostered the technological growth and refinement of Internet search processes. The mantle" of being
perceived by users as the most effective Internet aide provides Search Engine proprietors with the motivation to eradicate Meta tag abuse from their databases. It is proposed that Search Engines should be encouraged to devise advanced technological tools that can sift out trademarked words and / or phrases from the Meta tags within a web page. In this regard, an earlier proposal of Trademark tag deserves a careful analysis and a possible solution to Meta tag conundrum.

(2) To establish trademark infringement, it is necessary (other than in the case of dilution of a famous mark) for consumers to be confused as to the ownership of the mark or of the goods or services to which the mark is applied. Similarly, dilution of a mark depends on consumer perceptions. Most Internet-savvy users are unlikely to assume an affiliation between two linked sites, or products on those sites, particularly as the user leaves one site and travels to another upon clicking a hyperlink. It should, however, be remembered that users' perceptions will be influenced by the nature of the link. For example, if the linking site uses the linked site's fanciful logo as its pointer, consumers are more likely to believe that there is an association than if the linking site uses the address or name of the linked site as its pointer. It is, however, easy to prevent Search Engines from deep-linking to a specific page. All that is required is to insert the following Meta tag code in the HEAD part of the page:

\[
\text{<META NAME="robots' CONTENT="noindex">}
\]

Alternatively, cross-linking agreements and licenses can be explored between two parties permitting each party to hyperlink to the other's website in order to prevent dilution of trademark in cyberspace. Further, disclaimers can be added on the website prohibiting deep-linking of the web pages.

It is recommended that linking is a technology, which should not be tampered with lest it runs the risk of seriously undermining Internet's functionality and ease of use. However, in case of dilution of trademark through the use of links, courts are well equipped to determine if such a use causes confusion in the minds of the Internet users.
(3) Similarly, framing of a website can be prevented using a simple JavaScript Code in the HTML coding:

```javascript
<script type="text/javascript"><!
if (self != top)
{
    if (document.images)
        top.location.replace( window.location.href);
    else
        top.location.href = window.location.href; }
//--></script>
```

It is recommended that technology is well-equipped to address the techno-legal issues, like framing, that contribute towards trademark trafficking in cyberspace, and the use of such technologies should be encouraged.

2.7 Proposals to Address Jurisdictional Issues in Cyberspace

(1) Compliance with orders pertaining to international jurisdiction of courts in cases concerning trademark trafficking in cyberspace, it is submitted, will remain a utopian idea in the absence of international political consensus on the issue. At best, domestic courts can pass orders directing the administrative machinery managing the domain names on the Internet. ICANN has shown flexibility in this regard and given due consideration to the decisions of local courts during the proceedings under UDRP.

(2) National jurisdictional principles, however, have been dealt with at length by various U.S. courts and experts. From Zippo Sliding Scale analysis to Effects test, courts have dabbled with different formulations determining jurisdiction on the cases involving trademark violations on cyberspace. Zippo Sliding Scale analysis, though, seems acceptable for majority of the courts but there are some serious shortcomings in this analysis as well:

---

(i) The Sliding Scale analysis doesn't work in every instance. Chat room postings are classified by some courts as "passive". Characterising this act as passive does not result in a desirable outcome since the poster knows or ought to know that the effect of their posting will be felt most acutely in the home jurisdiction of the target: If the target is unable to sue locally due to a strict adherence to the passive versus active test, the law might be seen as encouraging online defamatory speech by creating a jurisdictional hurdle to launching a legal claim.

(ii) The Zippo test also falls short when active sites are at issue. While the active website may want to sell into every jurisdiction, the foreseeability of a legal action is confined primarily to those places where actual sales occur. The Zippo test does not distinguish between actual and potential sales, however, but rather provides that the mere existence of an active site is sufficient to assert jurisdiction.

(iii) The Zippo test inhibits e-commerce by effectively discouraging the adoption of interactive websites. Prospective website owners who are concerned about their exposure to legal liability will rationally shy away from developing active websites since such sites increase the likelihood of facing lawsuits in far-off jurisdictions. Instead, the test encourages passive websites that feature limited legal exposure and therefore, present limited risk. Since public policy aims are to increase interactivity and the adoption of e-commerce (and in doing so, enhance consumer choice and open new markets for small and medium sized businesses), the Zippo test acts as a barrier to that policy approach.

(iv) Majority of the websites fall into the "middle zone," which requires the courts to gauge all relevant evidence and determine whether the site is

---

61 Geist, infra, note 68
62 See, People Solutions, Inc. v. People Solutions, Inc., 2000 WL 1030619 (N.D. Tex., 2000), where the court's request for evidence of actual sales within the jurisdiction illustrates that the mere potential to sell within a jurisdiction does not necessarily make a website active
63 Geist, infra, note 68
64 Geist, infra, note 68
"more passive" or "more active." With many sites falling into this middle zone, their legal advisors are frequently unable to provide a firm opinion on how any given court might judge the interactivity of the website. Further, distinguishing between passive and active sites is complicated by the fact that some sites may not be quite what they seem. For example, sites that feature content best characterised as passive, may actually be using cookies or other data collection technologies behind the scenes unbeknownst to the individual user.\(^{65}\)

(v) The standards for what constitutes an active or passive website are constantly shifting. When the test was developed in 1997, an active website might have featured little more than an email link and some basic correspondence functionality. Today, sites with that level of interactivity would likely be viewed as passive, since the entire spectrum of passive versus active has shifted upward together with improved technology.\(^{66}\)

In order to overcome the shortcomings in the Zippo Sliding Scale analysis, Prof. Geist\(^{67}\) suggests targeting-based analysis, which, unlike Zippo, would seek to identify the intentions of the parties and to assess the steps taken to either enter or avoid a particular jurisdiction. The American Bar Association Internet Jurisdiction Project, a global study on Internet jurisdiction released in 2000, also recommended targeting as one method of addressing the Internet jurisdiction issue.\(^{68}\) Geist further contends that in order to identify the appropriate criteria for a targeting test, we must ultimately return to the core jurisdictional principle - foreseeability, which should not be based on a passive versus active website matrix. Rather, an effective targeting test requires an assessment of whether the targeting of a specific jurisdiction was itself foreseeable. Foreseeability in that context depends on three factors -

\(^{65}\) Id
\(^{66}\) Id
\(^{67}\) Professor Michael Geist, Is There A There There? Toward Greater Certainty For Internet Jurisdiction, 16 Berkeley Tech. L.J. 1345 (Fall, 2001)
\(^{68}\) Margaret G. Stewart, Achieving Legal and Business Order In Cyberspace: A Report On Global Jurisdictional Issues Created By The Internet, 55 Business Lawyer 1801 (2000) (reporter)
contracts, technology, and actual or implied knowledge. Forum selection clauses found in website Terms of Use

Agreements or transactional Click-Wrap Agreements allow parties to mutually determine an appropriate jurisdiction in advance of a dispute. It, therefore, provides important evidence as to the foresee ability of being hauled into the courts of a particular jurisdiction. Newly-emerging technologies that identify geographic location constitute the second factor. These technologies, which challenge widely held perceptions about the Internet's architecture, may allow sites to target their content by engaging in "jurisdictional avoidance." The third factor, actual or implied knowledge, is a catch-all that incorporates targeting knowledge gained through the geographic location of tort victims, offline order fulfilment, financial intermediary records, and Web traffic. While all three factors should be considered as part of a targeting analysis, the relative importance of each will vary. Geist concludes by underscoring the fact that "targeting analysis will not determine exclusive jurisdiction, but rather identify whether a particular jurisdiction can be appropriately described as having been targeted. The test does not address which jurisdiction is the most appropriate as between those jurisdictions that meet the targeting threshold.

The proposal endorsed by Prof. Geist is, hereby, recommended as a reasonable test to determine inter-state and/or inter-district jurisdiction in cases involving trademark trafficking in cyberspace.

2.8 Proposals to Improve UDRP Functioning

(1) Dispute resolution under ICANN UDRP is often criticised for promoting forum shopping. Therefore, in order to curb the menace of multiple dispute resolution service providers that compete amongst themselves, aiming to attract the most market share and driven by economic forces, there is a case for single Provider entrusted with the task of domain name dispute resolution. Further, the arbitrators should be monitored, ensuring quality in performance, and decision making. Such a system will also make it easier to establish a
uniform set of rules and legal precedents, resulting in more consistent findings based on law rather than an elastic rule stretched arbitrarily on a case-by-case basis.

(2) In order to eliminate chances of bias and ensure a fair decision, it is recommended that all contested UDRP actions should involve three-member panels. Establishing the three-member panel as the default would remove most Provider influence over Panellist selection and ensure better quality decisions by forcing Panellists to justify their reasoning to their colleagues on the Panel. As with the current system, both parties would play a role in selecting one Panellist, while the Provider would select the third Panellist from among a list that both parties have reviewed and accepted. Unlike the current system, the complainant would be required to cover the full cost of the three-member panel. Although such a measure will double the cost of a UDRP action for many complainants, the cost will still remain low in comparison with traditional litigation. In order to reduce complainant costs, it is further recommended to combine the mandatory three-member panel rule for contested cases with the FORUM's supplemental rule on respondent defaulta, which allows a complainant to move from a three-member panel to a single Panellist where the respondent fails to provide a response. In doing so, the complainant is refunded the difference in cost between a single and three-member panel.

(3) An appeal system within the UDRP mechanism is also recommended, which will further make the decisions rendered by the Panellists more consistent and accurate. Though it will make the process a little costlier, the party that loses the appeal may be made to bear the costs of appeal procedure

---

69 Rule 9(c), The National Arbitration Forum's Supplemental Rules To ICANN'S Uniform Domain Name Dispute Resolution Policy.