DYNAMIC INJUNCTIONS – INTERNET 'INJUNCTIONS 2.0'

Manmeet Kaur Sareen[*]

Kanika Kalra[**]

Abstract

Injunctions originated as a remedy in equity to render complete and effective justice. However, in the rapidly growing world of internet intermediaries, this remedy, in its existing form, is failing at rendering effective justice due to circumventive measures internet offers. Domain names or Uniform Resource Locators (URLs) can be ordered to be blocked or taken down if content on it is found to be objectionable. However, even after such injunctions are passed, the same content can surface the internet on new URLs or domain names which cannot be blocked by the injunction order as they are not included in the order.

Judicial dynamism has allowed for injunctions to be moulded to address complications that arise in individual cases, like the *John Doe* injunctions. Similarly, dynamic injunction is a new format of injunctions for tackling such circumventive measures adopted on the internet. In essence, a dynamic injunction is an injunction which acts as an order for blocking or taking down the infringing or objectionable content rather than just a domain name or URL, without imposing the obligation of monitoring or filtering content on the Internet Intermediaries. This paper aims at providing an understanding of the issues in implementing injunctions on the World Wide Web and analyses the ways in which dynamic injunction can be implemented in India.

I Injunction- A remedy in equity

II Injunctions in India

III Internet and intermediaries

IV Injunctions on intermediaries: An ineffective remedy

V Dynamic injunctions: A fair solution

VI Dynamic injunctions in the Indian context

VII Observations on dynamic injunctions in India

VIII Comments

IX Conclusion

I Injunction- A remedy in equity

EQUITABLE REMEDY is a non-monetary remedy, such as an injunction or specific performance, obtained when monetary damages cannot adequately redress injury.[1] Injunctions, as equitable remedies, were developed by the English Chancery Courts where

* Student, Faculty of Law, University of Delhi.

** Student, Faculty of Law, University of Delhi.

[1] Bryan Garner (ed.), *Black's Law Dictionary* (7th edn., 1999).

Chancellors directed a party to do or refrain from doing something.[2] The remedy of injunction filled the gaps where common law fell short. Traditionally, an injunction is a remedy which applies *in personam*[3] *i.e.,* it operates against the defendant(s) to the suit and not against a stranger or a third party[4] or a non-party.[5] The exceptions began with the passing of *John Doe* orders.

Thus, injunctions developed in order to:

1. Administer just, complete and equitable reliefs;
2. Cure deficiencies posed by the rigidities of common law and aid its growth;
3. Achieve maximum efficiency in the process of adjudication and decision-making.

II Injunctions in India

In India, the remedy of injunction is provided as a statutory relief in the Specific Relief Act, 1963 and the Civil Procedure Code, 1908 (hereinafter, 'CPC'). They are broadly categorized as temporary or permanent Injunctions. Interim injunctions are ancillary to the main relief which the plaintiff will be entitled to if he is successful in establishing a prima facie case and balance of convenience, and also if the court finds that the plaintiff will suffer irreparable loss and injury. The nature of a temporary injunction is protective with the objective of preventing any future possible injury[6] and to maintain *status quo* until final adjudication.

A permanent injunction, as the name suggests, continues forever under which the defendant is perpetually enjoined from the assertion of a right or from committing an act injurious to the rights of the plaintiff. It can be granted only after deciding the case on merits at the conclusion of the trial after hearing both the parties to the suit. Once a permanent injunction is granted, the temporary injunction ceases to exist separately and may merge into the decree of permanent injunction.

The objects of granting permanent injunction include:

- Preventing continuous injury and violation of legal right of plaintiff[7];
- Curtailing multiplicity of judicial proceedings[8] due to continuous violation;

---

[2] David W Raack,, "A History of Injunctions in England Before 1700", 61 (4) *Indiana Law Journal* 1(1986), *available at,* http://www.repository.law.indiana.edu/ilj/vol61/iss4/1. (Last visited on Dec. 8, 2019).

[3] *Prabhakara Adiga* v. *Gowri,* (2017) 4 SCC 97; *Board of Governors of Hospital for Sick Children* v. *Walt Disney Productions Inc,* [1968] Ch 52, (1967) 1 All ER 1005 (CA).

[4] *L.D. Meston School Society* v. *Kashi Nath,* AIR 1951 All 558; *Fakira* v. *Rumsukhibai,* AIR 1946 Nag 428; *Marwari Sabha* v. *Kanhaya Lal,* AIR 1973 All 298.

[5] *W.B. Housing Board* v. *Parmila Sanfui,* (2016) 1 SCC 743.

[6] *Polins* v. *Gray,* (1879) LR 12 ChD 438; *ITO* v. *M.K. Mohd. Kunhi,* AIR 1969 SC 430; *Manohar Lal Chopra* v. *Seth Hiralal,* AIR 1962 SC 527.

[7] R Yashod Vardhan and Chitra Narayan, *Pollock And Mulla : The Indian Contract and Specific Relief Acts* 2195 (Lexis Nexis,2nd vol, 15 edn., 2017).

- Providing equitable and complete relief to plaintiff where damages do not solely suffice;
- Preventing breach of an express or implied legal obligation existing in favour of defendant

Therefore, the remedy of injunction is provided to achieve maximum efficiency in rendering judicial decisions such that their practical application does not become ineffective.

While the remedies of injunctions are deeply ingrained in most judicial systems, the remedy has taken various *avatars* to adapt itself to the developments in societies and newer technologies. In such adaptation, traditional principles have become more flexible. For *e.g.,* in the case of *John Doe* orders, injunctions are granted even against unknown defendants, contrary to traditional understanding. The growth of the Internet has posed challenges to the judicial system to find newer ways to make injunctions more effective. The purpose of this piece is to analyse the challenges posed by the Internet in granting effective injunctive relief.

III Internet and intermediaries

The world wide web *i.e.,* the Internet is growing rapidly every millisecond. As of May-June 2018,

i. More than 300 million photos were uploaded every day, and every minute about 500,000 comments were posted and 293,000 statuses were uploaded on Facebook.[9]
ii. On Instagram, around 95 million photos and videos were shared each day.[10]
iii. the number of emails sent every minute were 156 million.[11]
iv. the number of videos viewed on YouTube per day were 5 billion and 300 hours of videos were uploaded per minute.[12]

In 2018, approximately 14,282 web sites were uploaded in one day.[13]

---

[8] *Ibid.*
[9] Bernard Marr, "How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read," *Forbes,* May 21, 2018, *available at,* https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#7f4e566660ba. (Last visited on Dec. 10, 2019)
[10] *Ibid.*
[11] *Id.*
[12] "YouTube By The Numbers: Stats, Demographics & Fun Facts", *Omnicore,* Jan. 6, 2019, *available at,* https://www.omnicoreagency.com/youtube-statistics/. (Last visited on Dec.20, 2019)
[13] "How Many Websites Are There Around The World?", *Mill For Business*, Feb. 2, 2019, *available at,* https://www.millforbusiness.com/how-many-websites-are-there/ (Last visited on Dec.20, 2019) (The number is based on authors' calculations.)

All these activities, such as creation of websites, uploading of pictures, videos, statuses etc. are performed with the help of Internet intermediaries.

Who are Internet intermediaries?

An intermediary is defined under section 2(w) of the Information Technology Act, 2000 as :

> "intermediary", with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, Internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes;

In other words, Internet intermediaries bring together or facilitate transactions between third parties on the Internet.[14] They give access to host, transmit and index content, products and services originated by third parties on the Internet or provide Internet-based services to third parties.[15]

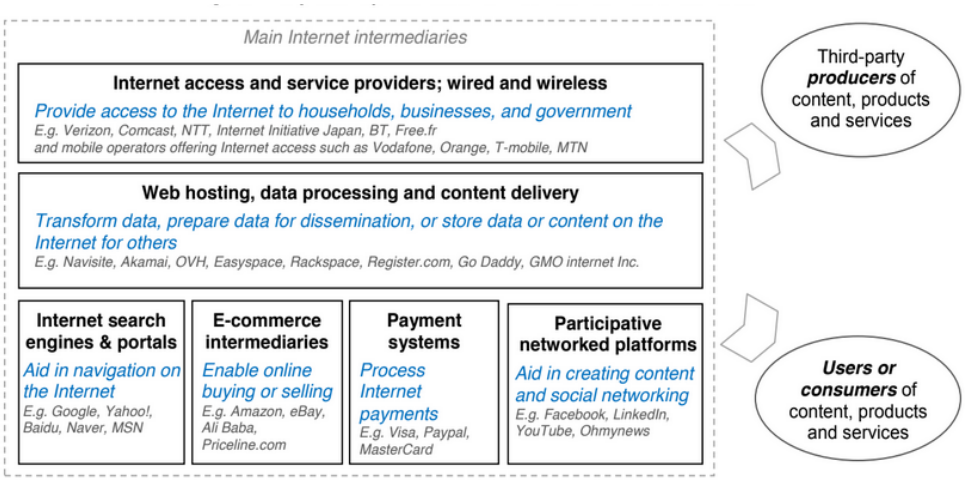

Figure: Stylised representation of Internet Internet Intermediary's roles[16]

So, for example, if 'A' creates a website, it is made accessible to public at large with the help of an Internet Service Provider (ISP) and is therefore an intermediary. If 'B' posts a video on

[14] Karine Perset, "The Economic And Social Role of Internet Intermediaries" *Organisation For Economic Co-Operation And Development,* Apr. 2010, *available at,* https://www.oecd.org/internet/ieconomy/44949023.pdf. (Last visited on Dec. 15, 2019*)*

[15] *Ibid.*

[16] *Ibid.*

YouTube; YouTube is the intermediary as it is the platform provider. Even if one simply searches for something on Google it is because Google is indexing content to facilitate the search which makes Google an intermediary.

Active intermediaries and passive intermediaries

Intermediaries are classified as active or passive for the purpose of fixing responsibility for content which is created and uploaded on the Internet through them. This classification is important for achieving the ends of adjudication at the time of fixing liability.

The different roles of intermediaries and their liability can be illustrated with the help of the following examples:

i. 'B' uploads a video on YouTube, an act by which A's copyright is being infringed. 'A' sues 'B' and YouTube for copyright infringement. The question is whether YouTube is liable for copyright infringement?

   'B' is the user, who is actually uploading the video and YouTube, being the platform provider, is facilitating the same.

ii. 'B' uploads a status on Twitter which can be categorized as a defamatory statement against 'A'. 'A' sues 'B' and Twitter for defamation. The question is whether Twitter is liable?

   Here again 'B' is the person who has uploaded a status on Twitter and expressed his opinion for the public to see and Twitter has provided 'B' with a way to make such opinions available to public at large.

iii. 'B' creates a website which is hosted on a server located in a foreign country. The said website is accessible in India through an ISP. The website helps users to download movies, over which 'A' has a copyright. 'A' sues 'B' and the ISP for copyright infringement. The question is whether the ISP is liable?

iv. 'B' posts a product for auction on eBay. 'A' purchases the product through the eBay platform. The product turns out to be counterfeit. A sues B and eBay. Is eBay liable?

In all these cases, the content is created by 'B' and the intermediaries are YouTube, Twitter, ISP and eBay respectively. Both are, in some way, contributing towards users being able to access the objectionable content. 'B' is dependent on the intermediary to provide him with a mechanism to upload his content for people to view it and the intermediary is also dependent on 'B' because its business model is dependent on content creators such as 'B'. So, both the

intermediary and the content creator are dependent on each other. The conduct which has been complained against would not have been possible if either one was absent.

Therefore, the questions that arise are:

i. Is only 'B' liable being the creator of the objectionable content?
ii. Is only the intermediary liable since it provided the mechanism for uploading such content and making it available to users?
iii. Are both liable?

As per the current position in law, an intermediary would be made liable only if it is characterized as an 'active' intermediary i.e. one who contributes in creation, transmission, modification etc. A passive intermediary is one that provides only a mechanism to upload content and does nothing more. Thus, in the above cases, the intermediaries would not be liable as they only provided a platform to upload content and did not actively engage in creating or transmitting content.

Passive intermediaries have been provided with the 'Safe-Harbor' defence under the E-Commerce Directive[17] passed by the European Union wherein intermediaries falling within Articles 12, 13 and 14 i.e. mere conduits, caching and hosting service providers respectively, were exempted from liability by virtue of Article 15. The Safe-Harbor defence was further elaborated by Courts in the celebrated decisions of *Google France*[18] and *L'oreal* v. *eBay.*[19] For other cases[20] like those relating to defamation, such exemption has also been referred to as 'innocent dissemination defence.'

The broad tests of the defences are similar. An exemption can be claimed if an intermediary is passive i.e. if it satisfies the following criteria:

i. **Knowledge criterion**: The intermediary must not have knowledge of the content that is uploaded on its platform unless it is informed.

[17] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society services, in particular Electronic Commerce, in the Internal Market (hereinafter, 'Directive on electronic commerce') [2000] OJ L178/1.
[18] *Google France SARL, Google Inc.* v. *Louis Vuitton Malletier,* SA C-236/08 to C-238/08 judgment of the court (Grand Chamber) Mar.23 2010.
[19] C-324/09, judgment of the court (Grand Chamber) July 12 2011.
[20] *Oriental Press Group Ltd* v. *Fevaworks Solutions Ltd.,* [2013] 16 HKCFAR 366.

ii. **Control criterion**: The intermediary must not be placed at a position from where it can exercise any sort of control over the content, like editorial control or control over the way the content is transmitted etc.

iii. **Expeditious removal after acquiring knowledge**: Once the intermediary obtains knowledge, in any manner, that certain infringing or objectionable content has been uploaded on its platform, it should act expeditiously in dealing with it because if it does not do so, it will be considered that the intermediary is aiding the dissemination of infringing or objectionable content.

If the intermediary is one which neither has knowledge nor control over the content and also has mechanisms to act expeditiously when it acquires knowledge, it will be exempted from liability.

In India, section 79 of the Information Technology Act, 2000 (hereinafter, 'the IT Act') exempts a passive intermediary from liability if it satisfies certain conditions that are broadly in sync with the abovementioned criteria. In order to be exempted from liability:

i. The function of the intermediary must be limited to provide a system for information transmission or hosting of information;
ii. The intermediary must not make any decision with respect to how and to whom information is transmitted;
iii. The intermediary must not modify content;
iv. The intermediary must observe due diligence [provided in the Information Technology (Intermediaries Guidelines) Rules, 2011 (hereinafter, 'Intermediary Guidelines')];
v. The intermediary must not aid, conspire or induce unlawful acts;
vi. The intermediary must act expeditiously once it obtains actual knowledge about objectionable content.

Most intermediaries like Facebook, YouTube, Twitter, Amazon, eBay *etc.* take the defence of being passive intermediaries and courts have generally exempted them from liability in cases where they have satisfied the required criteria for exemption. However, if courts find that the content is objectionable or infringing someone's rights, the courts may direct such intermediaries to remove or block such content from their platforms to render complete justice – this is where injunctions come in as an equitable relief. However, the existing

mechanism of injunctions is not proving to be entirely effective in cases involving Internet intermediaries.

IV Injunctions on intermediaries: An ineffective remedy

There are a number of cases where injunctions have been sought for violation of privacy, defamation, illegal streaming of copyrighted content, *etc.*, some of which are highlighted here under. Challenges posed in individual matters have led courts to pass varied kinds of orders to make injunctions effective. Confusion still persists as to what kind of order or injunction would be most effective in a certain scenario. In this section, we will briefly look at the current position in India and see how injunctions are proving to be an ineffective remedy in cases of violations on the Internet.

Injunctions are granted by directing intermediaries to remove or 'take down' or block certain content from being accessed. In order to get a domain name[21] or URL[22] blocked in cases where the content is defamatory or against public interest *etc*., the Plaintiff has to obtain an injunction order by a court directing the intermediary to block the domain name or URL. section 69A and 79 of the IT Act and certain rules[23] made under this Act form a part of the current regulatory regime in India. As per section 69A and the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 (hereinafter, 'Blocking Rules'), for certain cases pointed out in section 69A (1), there is a Designated Officer who will direct intermediaries to block certain content and the same can be done when a complaint is filed with a Nodal Officer or in furtherance of an order from a competent court. As mentioned above, for passive intermediaries, they can claim exemption from liability if they fulfill the required conditions in section 79[24] read with the intermediary guidelines. These were discussed and interpreted by Supreme Court in the decision of *Shreya Singhal* v. *Union of India.*[25]

---

[21] A domain name is an Internet resource name that is universally understood by Web servers and online organizations and provides all pertinent destination information. To access an organization's Web-based services, website users must know the precise domain name. *available at,* https://www.techopedia.com/definition/1327/domain-name (Last visited on Nov. 20, 2019)

[22] A uniform resource locator (URL) is the address of a resource on the Internet. A URL indicates the location of a resource as well as the protocol used to access it. *available at,* https://www.techopedia.com/definition/1352/uniform-resource-locator-url (Last visited on Nov. 30, 2019)

[23] Information Technology (Intermediaries Guidelines) Rules, 2011 *(hereinafter*, *Intermediaries Guidelines)* and Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 *(hereinafter*, *Blocking Rules)*.

[24] The Information Technology Act, 2000 (21 of 2000).

[25] (2015) 5 SCC 1.

In this case, the Supreme Court read down section 79(3) (b) and held that the term 'actual knowledge' in the section means notification by appropriate government agency or a court order. This interpretation was arrived at on the construction that section 79 is an exemption provision and was closely related to section 69A. The court found that section 69A read with Blocking Rules provided only two ways for blocking to take place *i.e.,* either by designated officer following the procedures prescribed in the rules or by designated officer on receipt of a court order; the method of an intermediary applying its own mind to decide whether or not a domain name or URL is to be blocked, is absent from section 69A. Therefore, on the conjoint reading of section 69A and section 79(3)(b), the latter was read down. Following are the relevant excerpts of the judgment:

> 116. It must first be appreciated that Section 79 is an exemption provision. Being an exemption provision, it is closely related to provisions which provide for offences including Section 69A. We have seen how Under Section 69A blocking can take place only by a reasoned order after complying with several procedural safeguards including a hearing to the originator and intermediary. We have also seen how there are only two ways in which a blocking order can be passed - one by the Designated Officer after complying with the 2009 Rules and the other by the Designated Officer when he has to follow an order passed by a competent court. The intermediary applying its own mind to whether information should or should not be blocked is noticeably absent in Section 69A read with 2009 Rules.

The court further observed :

> 117. Section 79(3)(b) has to be read down to mean that the intermediary upon receiving actual knowledge that a court order has been passed asking it to expeditiously remove or disable access to certain material must then fail to expeditiously remove or disable access to that material. This is for the reason that otherwise it would be very difficult for intermediaries like Google, Facebook etc. to act when millions of requests are made and the intermediary is then to judge as to which of such requests are legitimate and which are not. We have been informed that in other countries worldwide this view has gained acceptance, Argentina being in the forefront. Also, the Court order and/or the notification by the appropriate Government or its agency must strictly conform to the subject

> matters laid down in Article 19(2). Unlawful acts beyond what is laid down in Article 19(2) obviously cannot form any part of Section 79. With these two caveats, we refrain from striking down Section 79(3)(b).

The court summarized as under:

> 119. In conclusion, we may summarise what has been held by us above:
>
> (a) Section 66A of the Information Technology Act, 2000 is struck down in its entirety being violative of Article 19(1)(a) and not saved Under Article 19(2);
>
> (b) Section 69A and the Information Technology (Procedure & Safeguards for Blocking for Access of Information by Public) Rules 2009 are constitutionally valid;
>
> (c) Section 79 is valid subject to Section 79(3)(b) being read down to mean that an intermediary upon receiving actual knowledge from a court order or on being notified by the appropriate government or its agency that unlawful acts relatable to Article 19(2) are going to be committed then fails to expeditiously remove or disable access to such material. Similarly, the Information Technology "Intermediary Guidelines" Rules, 2011 are valid subject to Rule 3 Sub-rule (4) being read down in the same manner as indicated in the judgment;

Hence, by reading down section 79(3)(b) and rule 3(4) of the Intermediary Guidelines, it is now imperative for a person to either obtain a court order or complain to the Nodal Officer in order to get content taken down or blocked by an intermediary where the same is sought in furtherance of reasonable restrictions provided in article 19(2) of the Constitution of India.[26] However, the caveat left an open end to the interpretation of 'actual knowledge' for cases that did not pertain to article 19(2). Taking this into consideration, the Delhi High Court in *My Space* v. *SCIL*[27] held:

> In the case of copyright laws it is sufficient that MySpace receives specific knowledge of the infringing works in the format provided for in its website from the content owner without the necessity of a court order.

[26] The Information Technology [Intermediaries Guidelines (Amendment) Rules], 2018 has incorporated this read down position under proposed amended Rule 3(8). It is still pending. *available at,* https://meity.gov.in/writereaddata/files/Draft_Intermediary_Amendment_24122018.pdf (Last visited on Dec.10, 2019)

[27] 2017 (69) P.T.C 1 (Del).

By this decision, the necessity of obtaining a court order was eliminated but only for cases falling within the ambit of copyright laws.

In this case, MySpace had a specific format to receive knowledge about what is uploaded on their website, which could be resorted to directly in the opinion of the court. The high court observed that MySpace was filtering content providing for three safeguards on its platform, namely-

i. The Hash Block Filter which prevents the deleted content from being reposted by taking finger print of the content.
ii. Take Down Stay Down contents also prevents the repetitive reposting of the file containing identical content. Thus, the said filter is also a useful identifier for preventing repetitive infringement.
iii. Rights management tool is the most powerful filtering tool made freely available to copyright owners.

The court held that all these measures are nothing but safeguards to prevent infringement and sufficiently demonstrates their *bona fides* and non-involvement in the infringing acts.[28] However, not all platforms provide such mechanisms. Most social media platforms have their own policies and methods to tackle infringing and other objectionable content. In fact, all social media websites operating in India have to compulsorily provide for certain guidelines[29]. These guidelines and mechanisms are provided to deal with infringing, unlawful or objectionable content. For example: YouTube[30] provides for certain guidelines which the users are required to adhere to while posting videos. These pertain to harassment, bullying, copyright infringement, defamation, privacy, hate speech etc. They further give the option to users to 'flag' or 'report' content that is uploaded if it violates the standards. For tackling copyright issues, they also have the 'Content ID'[31] claim mechanism wherein they create a database of certain audio, video and other files given to them by copyright owners and scan audios or videos etc. against these for ensuring that there is no copyright infringement. They have also introduced 'Copyright Strike Mechanism' whereby a video is taken down by

[28] *MySpace* v. *SCIL,* 2017 (69) P.T.C 1 (Del).
[29] *Intermediary Guidelines,* Rules 3(1) and 3(2).
[30] *Policies and Safety,* (YouTube) *available at,* https://www.youtube.com/yt/about/policies/#community-guidelines (Last visited on Nov.25, 2019).
[31] *What Is A Content ID Claim,* (YouTube), *available at,* https://support.google.com/youtube/answer/6013276?hl=en&ref_topic=2778545 (Last visited on Nov.25, 2019).

YouTube if the copyright owner informs them that it is infringing his copyright and on getting three strikes there is a possibility that the infringer can never create a channel again.[32] Facebook[33] also works on community guidelines wherein users are advised not to upload content that may cause violence or promote crime, or content that promotes sexual violence or causes sexual solicitation, or promotes bullying and harassment, or pertains to hate speech, or violates intellectual property rights (IPR), or is false news, or is violative of someone's privacy etc. If such content is uploaded, a user has the option to report the content for it to be brought to the notice of Facebook. It also provides a form to complain against defamation. In the same manner, Twitter[34], Google [35]etc. also provide for similar guidelines and mechanisms to deal with objectionable, infringing or unlawful content.

Thus, different platforms have varying policies which govern their conduct. Most situations are taken care of by their policies, however, on a few occasions, there may be a divergence between the social media website and complainant as to whether, for example, content is actually infringing or not. It could be due to a simple reason such as registering the complaint with the intermediary under a wrong head. Sometimes, the website may be of the opinion that the conduct complained of is in a grey area and it cannot take a view on the matter, without impinging upon the rights of the defendant. In such cases a court order would be required. Further, after the decision of *Shreya Singhal (supra)* it has, in a way, become imperative for complainants to obtain court orders for various cases like defamation, immorality or indecent content, infringement of privacy etc. Therefore, to get a domain name or URL blocked, it is important to obtain an injunction order.

The requirement of a Court order is in furtherance of freedom of speech. This requirement brings the 'Reasonableness' within the 'Restrictions' by preventing over-blocking and curtailing excessive censorship by internet intermediaries in fear of litigation which may result in chilling effect on speech. However, these injunction orders may prove to be

---

[32] *Copyright Strike Basis,* (YouTube), *available at,* https://support.google.com/youtube/answer/2814000?p=c_strike_basics&hl=en. (Last visited on Nov.25, 2019).
[33] *Community Standards,* (Facebook), *available at:* https://www.facebook.com/communitystandards/ (Last visited on February 25, 2019).

[34] *Rules and Policies,* (Twitter), *available at:* https://help.twitter.com/en/rules-and-policies. (last visited on Dec.25, 2019).
[35] *User Content and Conduct Policy,* (Google), *available at:* https://www.google.com/+/policy/content.html. (Last visited on Nov.25, 2019).

ineffective because the content that has been taken down can be re-uploaded by a different domain name or URL. This can be done in various ways including the following:

i. **New username new URL**: User of a social media platform like Facebook can simply change his username[36] and upload injuncted content on that. This will have a new URL. This is same as saying a different user has uploaded it.

   Example: A user bearing username 'B' uploads a video on a social media platform Seebook, which impinging upon A's privacy. Its URL is https://www.seebook.com/watch?u=B12345. 'A' obtains an injunction order from the court and this URL is blocked. However later the same video is uploaded by user of account bearing username 'B' who changes his username to 'C'. This causes a change in URL – https://www.seebook.com/watch?u=C12345. This cannot be blocked by the injunction order as the new URL was not a part of that order.

ii. **Custom URL**: Websites like YouTube give an option of customizing your URL[37]. By fulfilling certain extremely simple criteria, a channel operator can customize its URL as he likes. If this is done even before the content is blocked, the new URL will automatically come out of the purview of the suit which was filed prior to changing of the URL.

   Example: 'B' uploads a video on YouSee which is defaming 'A'. YouSee provides customization of URL. The URL of the video is https://www.yousee.com/watch?u=AISbAd. 'A' files a suit praying for the URL to be taken down. 'B' then customizes the URL to https://www.yousee.com/watch?u=aAISbAdd which is possible to be done seconds after the suit is filed. In this scenario, the plaint and application for temporary injunction will have to amended to include the new URL.

[36] *How Do I Change My Username?* (Facebook), *available at,* https://www.facebook.com/help/162586890471598 (Last visited on February 25, 2019).
[37] *Get a Custom URL For Your Channel,* (YouTube), *available at,* https://support.google.com/youtube/answer/2657968?hl=en. (Last visited on Dec 25,2019)

There are many other ways of changing URLs even for entire websites. In *Department of Electronics and Information Technology* v. *Star India Pvt. Ltd.*[38] it was observed that changing URL is similar to changing a password and is an easy circumventing measure:

> 11. The steps to change a URL would require, to firstly access the source code of the infringing website and then change the alpha-numeric character string of the URL. This could be as easy as changing the password of one's e-mail Id. This would mean that if the URL of a rogue website is blocked, the operator can simply log into the website source code and change the URL akin to a person changing one's password. To give an example, a rogue website www.abc.com whose URL is www.abc.com/india-v-pakistan, can simply log into the website source code and insert the alphabet 's' after the alphabet 'v' and change the URL to www.abc.com/india-vs-pakistan. Thus, if the URL www.abc.com/india-v-pakistan is blocked, the infringer can start operating on the URL www.abc.com/india-vs-pakistan within a few seconds. But, if a domain name itself is blocked, to continue with the infringing activity becomes a cumbersome, time consuming and money spending exercise. A new domain name has to be created and purchased apart from purchase of *a fresh hosting server space. The entire exercise of creating a website has to be undertaken.*

iii. **Creating mirror websites**: A website owner can easily create a different website using the blocked content in a matter of minutes. It is the exact replica of a blocked website.

Example: *www.efg567.com* is a website which has certain content that infringes A's copyright. 'A' obtains an injunction order from court whereby all the ISPs are directed to block the domain name *efg567.com*. However, later another website is found by 'A', which is an exact replica of *efg567.com* and bears the domain name *zxy321.com*. The website is *www.zxy321.com*. This cannot be blocked by the injunction order as it was not included in the order.

iv. **Forwarding without masking** – Through this process the owner of the primary domain name can cause the user to be redirected or forwarded to the primary domain name by

[38] R.P.131/2016 in FAO (OS) 57/2015, High Court of Delhi, *available at,* http://lobis.nic.in/ddir/dhc/PNJ/judgement/29-07-2016/PNJ29072016REVIEWPET1312016.pdf (last visited on Dec.25, 2019)

creating a redirect domain name. What the address bar reflects is the primary domain name.

Example: The primary domain name owned by a person is efg567.com. While creating this domain name he also creates a redirect or forwarding domain name i.e. efgh5678.com. Now when a user searches for efgh5678.com, he is forwarded to efg567.com. The address bar[39] also displays efg567.com

v. **Forwarding with masking**: Through this process, the owner of the primary domain name creates a forward domain name through which user is redirected or forwarded to the primary domain name. Here the address bar will reflect the redirect or forward domain name since the creator has masked the primary domain name with the redirect or forward domain name.

Example: The creator of primary domain name *efg567.com* creates a redirect or forward domain name *efgh5678.com*. When a user enters *efgh5678.com* in the address bar he is automatically forwarded to *efg567.com*. In this case, since the creator has chosen to forward with masking, the address bar displays *www.efgh5678.com* though primary domain name is *www.efg567.com*. Since 'A' sees *www.efgh5678.com* in the address bar, he prays for blocking of *efgh5678.com* not realizing that the primary domain name is *efg567.com*.

Illustration of forwarding methods:

Forwarding **coolexample.COM** to **coolexample.NET**			
Forwarding Option	**Visitor Goes To**	**Site Visitor Sees**	**Address Bar Displays**
Forwarding Disabled	coolexample .COM	coolexample .COM	coolexample .COM
Forward w/o Masking	coolexample .COM	coolexample .NET	coolexample .NET

[39] An address bar is a component of an Internet browser which is used to input and show the address of a website. The address bar helps the user in navigation by allowing entry of an Internet Protocol address or the uniform resource locator of a website. It can also save previously used addresses for future reference, *available at*, *https*://www.techopedia.com/definition/5336/address-bar (last visited on Dec. 1, 2019).

Forward w/ Masking	coolexample .COM	coolexample .NET	coolexample .COM

Source: GoDaddy [40]

The above mentioned examples were a way to illustrate the different ways in which the exact same content can be re-uploaded or re-published on the Internet. If the Plaintiff obtains an injunction whereby an intermediary is directed by the court to block a specific domain name(s) or URL(s), the same content can reappear in a matter of seconds but since it bears a new domain name or URL it cannot be blocked by the earlier injunction order as the new domain name or URL was not a part of the earlier order. This can happen during or after the dispute. Taking the above examples, if the Plaintiff obtains a temporary injunction order whereby court directs intermediary to block a specific domain name(s) or URL(s) until final decree is passed, the same content can be uploaded again by the above-mentioned methods while the dispute is pending. It can even be done as soon as an Application under Order 39, CPC is filed but before the temporary injunction can be granted. So, the new URLs cannot be blocked until they are mentioned in the injunction order. The same can happen even after permanent injunction is granted.

Therefore, the same content can be seen using different names. Thus, the Internet gives effect to the old proverb '*All Roads Lead to Rome'*.

The problems associated with this are:

i. **Distress to the plaintiff**: If the Plaintiff finds the new URL(s) or domain name(s) after obtaining a permanent injunction over previous specified URL(s) or domain name(s) with the same content, a new suit would have to be filed to get the new URL(s) or domain name(s) blocked as the new URL(s) or domain name(s) was not a part of the previous order. If the Plaintiff finds the new URL(s) or domain name(s) during the pendency of the dispute, fresh applications for temporary injunctions would have to be filed increasing the burden on the Plaintiff.

ii. **Multiplicity of proceedings**: Since the Plaintiff is required to file a new suit, it leads to multiplicity of proceedings.

[40] *Manually Forwarding or Masking Your Domain or Subdomain,* (GoDaddy), *available at,* https://in.godaddy.com/help/manually-forwarding-or-masking-your-domain-or-subdomain-422 (Last visited on Dec.2, 2019).

iii. **Delay in getting justice**: If new URL(s) or domain name(s) come up during the dispute, applications under Order 39 of CPC have to be filed by the Plaintiff time and again to get new URL(s) or domain name(s) blocked causing delay in finally adjudicating the case.

iv. **Ineffective injunctions**: As discussed above, injunctions developed as equitable reliefs to give effective and complete justice and eliminate the deficiencies in common law. However, in injunctions involving the Internet, multiple means are available to by-pass the injunction. Finality in adjudication cannot be reached because the injunction is not on the content but on the URL or domain name. This means that what is blocked is the URL or domain name and not the content *per se,* which can resurface on the Internet. Hence, the injunction becomes ineffective.

Further, it has been observed that monitoring each and every post is practically impossible and highly costly.[41] However, imposing obligations on the intermediaries to filter content in the arena of copyright infringement as a statutory directive was being debated and discussed in the European Union. Article 13 of the Proposal for a Directive of the European Parliament And of The Council on copyright in the Digital Single Market[42] was a subject of great debate and critique as it is suggestive of the intermediaries being saddled with the obligation of putting in place content monitoring, filtering and scanning systems.[43] The directive has been recently passed.[44] In effect, this implies that the social media platform will be liable for the copyright infringing content uploaded on its platform.

V Dynamic injunction: A fair solution

Under these circumstances, judicial dynamism has led to the concept of `Dynamic injunctions' being developed. European Commission defines dynamic injunctions as:

---

[41] *MySpace Inc* v. *Super Cassettes Industries Ltd* 2017 (69) PTC 1 (Del); Jacqueline D. Lipton, "Law of the Intermediated Information Exchange", 64 *Florida Law Review* 1337 (2012).

[42] European Commission, "Proposal For A Directive Of The European Parliament And Of The Council On Copyright In The Digital Single Market, Brussels", (14 September 2016), *available at,* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016PC0593&from=EN (Last visited on January 30, 2019)

[43] Mason Sands, "Who Article 13 Really Hurts And Helps*", Forbes*, February 18, 2019, *available at:* https://www.forbes.com/sites/masonsands/2019/02/18/who-article-13-really-hurts-and-helps/#65c1f1376666. (last visited on Dec.20, 2019)

[44] Rhett Jones, "*A*' Dark Day': Copyright Law That Threatens The Internet As We Know It Passes Final EU Vote"*, Gizmodo*, March 26, 2019, *available at*: https://gizmodo.com/a-dark-day-copyright-law-that-threatens-the-internet-a-1833570802. (Last visited on Dec. 22, 2019).

> injunctions which can be issued for instance in cases in which materially the same website becomes available immediately after issuing the injunction with a different IP address or URL and which is drafted in a way that allows to also cover the new IP address or URL without the need for a new judicial procedure to obtain a new injunction.[45]

It further refers that –

> "the possibility of issuing such injunctions exists, inter alia, in the United Kingdom and Ireland. This objective could also be pursued through intervention of a public authority or the police…"[46]

A dynamic injunction is essentially an injunction which acts as an order for, in a way, blocking the infringing or objectionable content rather than just a domain name or URL. If a Plaintiff obtains a dynamic injunction with respect to certain domain names and/or URLs, it implies that he no longer has to again approach the court if the same content appears on a different domain name or URL; the injunction order blocking the initial domain name or URL will also be applicable for the new domain name or URL. Courts in various countries have passed express or implied dynamic injunctions.

Singapore

The High Court of Singapore expressly granted a dynamic injunction in the case of *Disney Enterprises, Inc.* v. *M1 Ltd.*[47] The plaintiffs in this case were copyright owners of numerous cinematograph films. They had been granted blocking orders under section 193DDA of the Copyright Act and the defendants (ISPs) were directed to take steps to block the identified FIOLs (Frequently Infringing Online Locations) i.e. the domain names, IP Addresses and URLs providing access to infringing content. The Plaintiffs had also prayed for a dynamic injunction. The court granted the same based on the following findings[48]:

[45] Communication From The Commission To The European Parliament, The Council And The European Economic And Social Committee, "Guidance on certain aspects of Directive 2004/48/EC of the European Parliament and of the Council On The Enforcement of Intellectual Property Rights*"* (Brussels, 29 November 2017).
[46] *Ibid.*
[47] (2018) SGHC 206.
[48] *Ibid.*

i. The court held that a dynamic injunction anticipates and seeks to counteract circumventive measures that may be taken by owners or operators of the FIOLs which would include measures taken to change to the domain name, URL and/or IP address providing access to the FIOL. Following example was given by the Court:

> For example, the primary domain name for the FIOL "*xmovies8"* has since been changed from "*xmovies8.es*" to *"xmovies8.nu*". As the domain name "*xmovies8.nu*" did not exist at the time of the application and was not listed under the plaintiffs' schedule, should the dynamic injunction not be granted, the plaintiffs would need to apply to the court to amend the main injunction in order to add the new domain name for it to be blocked. On the other hand, the dynamic injunction would remove the need for the plaintiffs to return to court to apply for an amendment of the main injunction or for a new order.

ii. With respect to the question regarding jurisdiction of the court to grant a dynamic injunction, the court stressed on the fact that nothing under section 193DDA precluded the court from granting a dynamic injunction. It observed:

> 38**.** I found that the court has the jurisdiction to issue a dynamic injunction given that such an injunction constitutes "reasonable steps to disable access to the flagrantly infringing online location". This is because the dynamic injunction does not require the defendants to block additional FIOLs which have not been included in the main injunction. It only requires the defendants to block additional domain names, URLs and/or IP addresses that provide access to the same websites which are the subject of the main injunction and which I have found constitute FIOLs (see [19] Â [29] above). Therefore, the dynamic injunction merely blocks new means of accessing the same infringing websites, rather than blocking new infringing websites that have not been included in the main injunction. [49]
>
> ……
>
> 40. Further, while s 193DDC of the Copyright Act provides a mechanism for the variation of the main injunction, I agreed with the Plaintiffs' submission that this did not preclude the court from issuing a dynamic injunction in the

[49] *Ibid.*

original order. [50]

The court also stressed on the legislative object of section 193DDA while granting the dynamic injunction and held[51]:

> 53. Such an approach was, in my view, consonant with the legislative objective of section 193DDA of the Copyright Act which is to provide a means of disabling access to the FIOL, given the nature of online piracy today including the ease with which circumventive measures may be adopted.

iii. The following benefits of dynamic injunctions were pointed out by the court[52]:

a. The main injunction order operates effectively;

b. Further harm to Plaintiffs is reduced;

c. Measures for circumventing injunction can be taken quite quickly and easily by operators of FIOL;

d. Without a continuing obligation to block additional domain names, it would be unlikely that there would be effective disabling of FIOL;

e. The dynamic injunction could potentially reduce the burden on the defendants as they would not have to indulge into litigation by responding to Plaintiffs' application for variation of the main injunction every time a new FIOL is found.

The Court held that "a dynamic injunction provides a practical means of ensuring continued effectiveness of the original injunction since it provides an expedited process for the blocking of additional FQDNs (Fully Qualified Domain Names - this includes domain names, IP addresses and websites) which resolve to the same infringing websites, where this is undisputed and unchallenged by the defendants."

The dynamic injunction was granted with a proviso to the effect that if the Intermediary felt that sufficient grounds did not exist for blocking, it could refuse to block. The defendant could also challenge the request for blocking. The relevant excerpts are as follows[53]:

[50] *Ibid.*
[51] *Ibid.*
[52] *Ibid.*
[53] *Ibid.*

> 44. Further, in order to ensure that the interests of the defendant network service providers are not unduly impinged by the dynamic injunction, I included a proviso in the order granted, along with the liberty for parties to apply. Under the proviso, the defendants would not be required to block the additional FQDNs upon the request of the plaintiffs if they are of the view that the grounds for disabling access provided by the plaintiffs are insufficient….
>
> ….
>
> 50. …The defendants and owners of the online locations remain free to challenge the plaintiffs' attempts to block additional FQDNs under the express terms of the order, and also pursuant to s 193DDC of the Copyright Act.

The following was the procedure laid down by the court for effective implementation of dynamic injunctions[54]:

i. Whenever Plaintiff acquires knowledge about additional FQDN(s) via which FIOL(s), blocked through main injunction, is accessible, he will inform the defendant in writing from time to time;
ii. Plaintiff will also provide an affidavit along with evidence to the Defendant and the Court mentioning the additional FQDNs and the reasons supporting the fact that they are providing access to the FIOLs blocked in the main injunction;
iii. Defendants are required to take reasonable steps within 15 working days of getting the notification/affidavit and disable the access to the additional FQDNs which made identified FIOLs accessible;
iv. Proviso- If defendants are of the opinion that the grounds given for disabling access to any of the FQDNs are insufficient, the defendants are not obligated to disable the access but are required to notify the Plaintiffs about the reasons for not disabling access within 15 working days of the receipt of the affidavit.

Based on this mechanism of dynamic injunction, it seems to be a fair solution because this measure not only relieves the Plaintiff from repeatedly approaching the Court, but at the same

---

[54] *Ibid.*

time it also ensures that the interest of the intermediaries is not unduly hampered.

While rendering this decision the Court considered the UK and Australian approach towards dynamic injunction. While considering the UK approach, the Court referred to the decision in *Cartier International AG* v. *British Sky Broadcasting Ltd.*[55] where the following was observed:

> 14. An important feature of all of the orders made pursuant to s.97A has been that they have included a provision for the right holders to notify additional IP addresses or URLs to the ISPs in respect of the websites which have been ordered to be blocked. This has allowed the right holders to respond to efforts made by the website operators to circumvent the orders by changing their IP addresses or URLs. Responsibility has fallen on the right holders to identify IP addresses and URLs which are to be notified to ISPs in this way.

The Court further considered the Australian decision in *Roadshow Films Pty Limited* v. *Telstra Corporation Ltd.*[56] where the Court while granting an injunction, held that if Plaintiffs want to get additional domain names, URLs or IP addresses blocked on the ground that they are the same online locations against which injunction has been granted, they will be required to obtain an order from the Court.

The Singapore High Court found that the Australian Court may have taken this approach to prevent over blocking. This, in the opinion of the Singapore High Court, was an overstated concern as through the proviso in its order it had been fair to the defendants i.e. the intermediaries.

Milan

Milan Court of First Instance (*Tribunale di Milano*) granted a dynamic injunction against ISPs in a case filed by Mondadori Magazine on the ground of copyright infringement. In the opinion of the court if an injunction could not operate in the future and Court intervention is required again, it would render the injunction pointless and would be contrary to the purposes of injunction.[57]

[55] [2017] 1 All ER 700.
[56] [2016] FCA 1503.
[57] Eleanora Rosati, "Milan Court Issues Dynamic Blocking Injunction Against Italian ISPs", *IPKat Blog,* August 25 , 2018, *available at:* http://ipkitten.blogspot.com/2018/08/milan-court-issues-dynamic-blocking.html (last

VI Dynamic injunctions in the Indian context

In India, dynamic injunctions have not been granted expressly as yet. However, certain important observations have been made in various orders which in our opinion support the concept of granting dynamic injunctions. Some of them are as follows:

i. *Tata Sky Ltd.* v. *YouTube LLC*[58]

In this case, Tata Sky had submitted a complaint to YouTube using the 'report' option provided by YouTube requesting it to take down certain URLs which provided instructions on how to hack the Tata Sky HD Set Top Box to receive High Definition content free of cost. There was confusion as to which head the complaint should be categorized into.

Correspondence was exchanged and finally YouTube told Tata Sky to file a copyright complaint after which Tata Sky filed the suit praying for an injunction against YouTube against unauthorized use of Tata Sky trademark and also from posting, screening or providing any audio or video material which seeks to provide or inform any methodology to hack into the Tata Sky system.

The court had granted an injunction initially and YouTube had taken down the content. Tata Sky still alleged that it was aggrieved by the delay in YouTube's response to complaints of Tata Sky which caused many people to hack into HD channels and view them for free. The court observed[59]:

> 24. With the URLs of the offending video in the instant case having been taken down by YouTube, and with its statement that those URLs will not hereafter be permitted to continue on the website of YouTube LLC, the interim injunction granted by the Court has worked itself out as far as YouTube is concerned. It is clarified that the said injunction order was directed at it not because YouTube had violated any trademark of Tata Sky but because its website hosted the offending URLs which required to be taken down. It was for that purpose alone that

visited on Dec. 2019) (present piece explains the case in English language with a good comment and becomes primary read for this case as the primary case originally is in Italian language*)*.

[58] 2016 SCC OnLine Del 4476

[59] *Ibid.*

> YouTube was a necessary and proper party without whose compliance the injunction order would have not been able to be implemented. With YouTube assuring that if there is any further complaint of a similar nature by the Plaintiff, YouTube LLC will not be found wanting in responding immediately to take down any such similar offensive material consistent with the interim injunction issued by the Court on 27th August 2015, the Court does not consider it necessary to dwell on the issue further. The interim injunction is made absolute against all other 'unknown' defendants.[60]

The injunction granted in this case was similar to a dynamic one because the court held that YouTube i.e. the intermediary will not wait and immediately take down content when Plaintiff makes a complaint of a similar nature which is consistent with the injunction order.

ii. ***Balaji Motion Picture Limited* v. *Bharat Sanchar Nigam Ltd.*[61]**

In this case, the Plaintiff sought a *John Doe* order against Defendants in order to restrain rogue websites infringing its copyright over the movie UDTA PUNJAB. The court did not grant an order directing websites to be blocked but allowed for specific URLs to be taken down. Relevant excerpts are reproduced as under[62]:

> 13. It is stated on behalf of the Plaintiffs that in advance of the film's release tomorrow, 17th June 2016, the Plaintiff has found that illicit pirated copies of the film apparently have already been available on some sites. A list of these is tendered. This list is taken on record and marked "X" for identification. The list given to me today contains not just the URL or domain name of the websites but the URL of the actual download links. There is no doubt in my mind that these links must all be removed or rendered inaccessible. Therefore, in addition to the foregoing order, there will also be an order in favour of the Plaintiff directing the Defendants and all other person to immediately remove these links, a list of which is appended to this order and all other links to any unauthorised downloads of this film. I am also informed that portions of the film were in fact being made available on YouTube. This material has now been removed.

[60] *Ibid.*
[61] 2016 SCC OnLine Bom 6607.
[62] *Ibid.*

> **14.** Where necessary, the local Police Authorities are directed to render all possible assistance to the Plaintiff in the enforcement of this order.
>
> **…**….
>
> 16. Should the Plaintiff find any actual instance of piracy or infringement, including on a secure website, the Plaintiff will be at liberty to apply without notice.
>
> **17.** ……The internet service providers cannot be expected to police the Internet or to monitor the contents of every single website. They only provide connectivity. Internet service providers, like all intermediaries, have sufficient statutory protection. I have no doubt that if and when the Plaintiffs draw attention to any of these intermediaries or cable operators to any site that contain illicit material, those intermediaries and cable operators will undoubtedly cooperate as they are required to do under the statute. [63]

This order also indicated that for an injunction to be effective, Plaintiff should be able to approach the defendant directly who in turn should reasonably cooperate.

iii. *Patanjali Ayurved Limited* v. *Google LLC*[64]

In this case that Plaintiffs alleged that video on the website of the defendants was defamatory and threatening and should be removed. The court found the following:[65]

> 9. The video clearly is violative of the above guidelines which Google and Youtube have prescribed for themselves. The video is also not just offensive against the Plaintiffs but could border on threats constituting violations of law. Defendants No.1 and 2 have therefore rightly removed the video from their platforms. Facebook Inc. (Defendant No.3) is also directed to ensure that the links to the said video links are no longer made available on its platform.
>
> 10. If there are any further instances of the same video being uploaded, which come to the knowledge of the Plaintiffs, in view of the above findings of the

[63] *Ibid.*
[64] 2019 SCC OnLine Del 7362.
[65] *Ibid.*

> Court, the Plaintiffs are permitted to intimate the Defendants and the Defendants shall take down the video within 48 hours. Having heard the submissions of the parties and in view of the stand taken by Google and YouTube, since the video itself has now stated to have been taken down not just on the India domain but from all the international platforms of Google and YouTube no further orders are required to be passed in the present suit.[66]

Again, by this decision the court ordered that the Plaintiff should approach the intermediary directly if the same video, over which injunction is granted, is found again on the platform and the defendant in turn should take it down pursuant to the injunction already granted.

VII Observations on dynamic injunctions in India

Dynamic injunction is a way of making injunctions granted by courts effective in the World Wide Web. In our opinion, a dynamic injunction method is not just a requirement at the end of the adjudication *i.e.,* as a permanent injunction but also during adjudication i.e. as a temporary injunction so that there can be timely and effective adjudication of the dispute. Further, it should not just be confined to the cases of copyright or IPR infringement but should cover all cases where an injunction is granted by a court, be it defamation, hate speech and other similar issues.

In order to expressly grant dynamic injunctions in an effective manner, there is a need that a mechanism is put in place for the same. The questions that are required to be answered are:

i. Whether intermediaries can be empowered to assess if a new domain name or URL should be blocked without the order of a Court?
ii. Whether complaint can be directly addressed to the intermediary or is there a requirement of involving a government agency or some other person to whom the complaint about new domain names or URLs can be addressed?
iii. Whether new domain names or URLs can be blocked based on the injunction order that has already been granted when the content on the new URLs or domain names is not same, but similar? If so, what should be the extent of similarity between the content on blocked domain names or URLs and the new domain names or URLs?

[66] *Ibid.*

iv. Whether there is a need to involve a governmental agency to ensure compliance of such orders and also make sure there is no over-blocking?
v. Whether a dynamic injunction should be statutorily incorporated?

It is true that there is a possibility of certain negative effects of a dynamic injunction like over-blocking or incorrect assessment of content leading to fair content being blocked etc. However, in our opinion the positives do outweigh the negatives and if a mechanism is put in place then the negative effects can also be avoided.

We need a system of dynamic injunction because effective adjudication is being hindered due to the sheer volume of content, the speed at which it is uploaded and the circumventive measures that are being adopted. It is proving to be difficult to carry out effective adjudication as can be seen in *Pepsico India Holdings Private Ltd.* v. *Facebook.*[67] The Plaintiffs filed a suit with an application for temporary injunction alleging that a video by an anonymous person on the website of the defendants baselessly and recklessly showed the Plaintiff's product i.e. LAY's chips, in bad light. On Feburary 23, 2018 Delhi High Court granted a temporary injunction in favour of the Plaintiffs with the following direction[68]:

> Till the next date of hearing, the defendants will take steps to block the URLs/ weblinks or any other similar video which are mentioned at pages 4 to 7 of the list of documents filed by the plaintiff.

On July13,2018 the order dated February 23, 2018 was amended in the following manner:

> The above direction (dated 13.07.2018) to the effect of seeking to block URLs/WebLinks regarding "any other similar video" shall remain suspended.
>
> In the eventuality, the plaintiff were to find any similar videos as stated in order dated 23.02.2018 liberty is granted to the plaintiff to approach the court.

Presently, settlement negotiations are underway in the matter. The matter is still pending.

[67] CS(OS) 80/2018, High Court of Delhi.
[68] *Ibid.*

VIII Comments

In our opinion, there is definitely a requirement for a mechanism like dynamic injunction to be established to make sure that circumventive measures adopted on the Internet do not hamper the efficiency of the adjudication process and that law keeps pace with the growth of Internet. It is a fair method because it aids the plaintiff, reduces burden of the court and does not impose undue obligations on the defendant.

The possible answers in our opinion to the above questions can be as follows:

Answer to questions 1 and 3:

Intermediaries and ISPs can be directly informed about the new domain names or URLs and in cases where the content on the new domain names or URLs is identical to that content against which injunction has already been obtained, the same can be assessed and removed by the intermediary. Under the Intermediary Guidelines in cases where the affected person complains of violation of sub-rule 2 of rule 3 the intermediary is required to take action within 36 hours on receiving actual knowledge by the affected person under Rule 3(4), which has been read down by the decision in *Shreya Singhal (supra)*. Further, by virtue of sub-rule 5 an intermediary is required to publish the name and contact details of the Grievance officer on its website who is required to redress complaints of users facing violation of rule 3 within one month.

So, in cases of dynamic injunctions the Plaintiff can address a complaint to the intermediary itself which will only be required to see whether or not the content is the same. Following the approach laid down by the High Court of Singapore, the Plaintiff should be required to give/file an affidavit to the intermediary and court stating the domain name or URL that it seeks to block along with evidence showing that the new domain name or URL provides the same content as was there in the blocked domain name or URL. If the content is the same, the intermediary should be bound to block it by virtue of the dynamic injunction that has already been granted. If not, then it should notify with the plaintiff the reasons for not blocking, and the remedies to both parties would be left open. This can at least help in removing the same content through different URL, redirect or masked websites.

Answers to 2 and 4:

Alternatively, a governmental agency can be directed to receive the complaint of the Plaintiff after a dynamic injunction has been granted and ensure effective compliance of the order. In the case of *Department of Electronics and Information Technology (DEITy)* v. *Star India Pvt.*

Ltd.[69] the Single Judge of the Delhi High Court had ordered for blocking of certain rogue websites which were violating Star India's exclusive license of media rights in various sporting events and issued a direction to *DEITy* to ensure compliance. *DEITy* appealed against the latter direction and vide order dated 10.03.2016 the Division Bench restricted the scope of the injunction by the Single Judge to the extent that only specific URLs will be blocked and not the entire website. The Court also recorded that a body, CERT-In[70], had been constituted to block specific URLs amongst its other functions. Later, a review petition was filed where the Court realised that URLs could be easily changed and therefore there was a need to block the entire website. Therefore, Single Judge's order was restored. Following was an observation made by the Court[71]:

> **15.** On the issue of whether the appellant could be directed to ensure compliance with the blocking order directed against the service providers, suffice it to state that it is the duty of the Government, its instrumentalities and agencies to assist in the enforcement of orders passed by the Courts.

The main provision by which a governmental agency is required to block content based on court orders is Rule 10 of The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009. By virtue of this provision the Designated Officer as under Rule 3 shall submit the certified copy to the Department of Information Technology and initiate action directed by the Court. However, the only issue here is that since these Rules have to be read conjointly with section 69A, such measures can be taken for cases provided in section 69A(1) which does not cover all cases like copyright or other IPR infringement.

The DIPP[72] has recently published the Draft on National e-Commerce Policy[73] whereby it has made the following recommendations with respect to online piracy:

> (D) Anti-piracy measures

---

[69] R.P.131/2016 in FAO (OS) 57/2015, High Court of Delhi, *available at:* http://lobis.nic.in/ddir/dhc/PNJ/judgement/29-07-2016/PNJ29072016REVIEWPET1312016.pdf (last visited on Dec.20, 2019).

[70] The Indian Computer Emergency Response Team. CERT-In has been incorporated in The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 by virtue of S. 70B of the IT Act. R. 9 of these rules provide the main functions of CERT-In which mostly pertain to cyber security incidents.

[71] *Supra* note 69.

[72] Department of Industrial Policy and Promotion.

[73] Department of Industrial Policy and Promotion, *Draft National e-Commerce Policy India's data for India's Development* (Feb. 23, 2019), *available at:* https://dipp.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf (last visited on Nov.28, 2019).

> Online distribution of pirated content is a matter of serious concern. The following are strategies proposed to be put in place to tackle this.[74]
>
> 3.18 Intermediaries shall put in place measures to prevent online dissemination of pirated content. Intermediaries shall identify 'trusted entities', whose complaints are resolved on priority. The identification of trusted entity and anti-piracy measures shall be done on a voluntary basis.
>
> 3.19 Upon being notified by the owner of copyright protected content/ work that a website or e-commerce platform is making available, selling or distributing the copyrighted content/ work without the prior permission/ authorization of the owner, such website or platform should expeditiously remove or disable access to the alleged content.
>
> 3.20 A body of industry stakeholders will be created that shall identify 'rogue websites'. Rogue website would refer to those that host predominantly pirated content. After verification, these rogue websites shall be included in the 'Infringing Websites list'. This shall invite the following:
>
> a) Internet service providers shall remove or disable access to the websites identified in the IWL within set time-lines.
>
> b) Rogue websites earn their revenues through online payments made based on a subscription or advertisement revenue models. Such payments have to be routed through Payment Gateways, which shall not permit flow of payments to or from such rogue websites.
>
> c) Search Engines shall take necessary steps to remove websites identified in the IWL, in their search results
>
> d) Advertisers or advertising agencies shall not host any advertisements on the websites identified in the IWL.

This draft does not only require constitution of a body to assess infringement but is also imposing an obligation on the intermediaries. In our opinion, such a body can be made for implementing dynamic injunctions, even in cases other than copyright infringement.

Answer 5:

[74] *Ibid.*

Over the years, injunctive reliefs have shown their dynamism in how they can be easily moulded with changing scenarios and applied in the best possible way, like in the form of *John Doe* injunctions. According to us, the various flexibilities in the forms and manner of granting injunctions are not required to be expressly incorporated in a statute. However, we do believe that the intermediary guidelines can be amended to incorporate implementation of dynamic injunctions by intermediaries.

IX Conclusion

Injunctions were originally introduced as a remedy to eradicate the shortcomings in the reliefs provided under common law. The gaps between adjudication and implementation were bridged. Slowly as society developed and complexities arose, the forms of injunctions also developed from being a remedy *in personam* to becoming a remedy *in rem.* The most recent example of such change is the *John Doe* or the *Ashok Kumar* injunction orders. Another example of the same is given under section 25 of the Delhi Rent Control Act, 1958 by which an order made by the controller for recovery of possession is made binding on all persons who may be in occupation of the premises and vacant possession thereof is to be given by any such occupant to the landlord. Such an order is binding on any party who is in possession even if that party is not the defendant. In other words, the remedy of injunction is of a dynamic character in itself and it has been modified to adapt to the requirements of the case in the changing scenarios.

Internet intermediaries and their business models are posing a real challenge to the effectiveness of injunctive reliefs due to the technological means adopted by defendants. There have been judgments by Courts in India for individual cases where different approaches have been adopted to address such challenges posed by intermediaries. For example, in the case of *Sabu Mathew* v. *Union of India*[75] a Nodal Agency and expert committee was created to address the issue of advertisements displayed on the websites of search engines like Google, Yahoo, *etc.* contravening section 22 of Pre-conception and Pre-natal Diagnostic Techniques (Prohibition of Sex Selection) Act, 1994. The apex court directed the search engines to install and apply 'auto-block' mechanism. However, since filtering and monitoring is not done in each and every case, the general relief of injunction for such cases is still ineffective.

[75] (2017) 2 SCC 514 read with (2018) 3 SCC 229.

The main purpose for developing injunctions as a relief was for increasing the effectiveness of implementation of remedies, which is being lost when the same is imposed on Internet intermediaries. In our opinion, a dynamic injunction is a step towards acclimatising the judicial system to the Internet and circumventive measures adopted on it so that decisions rendered are effective. It is simply a modified way of granting and implementing injunctions. A dynamic injunction helps in removing the same content on a different URL. It is not circumventing the existing imperative requirement of obtaining a court order. At the first instance, a court order is still required to be obtained. Dynamic injunction is only increasing the power of the injunction order and aiding the plaintiff by saving him time, cost and effort of unnecessarily undertaking another litigation for essentially the same problem. Further, as we have already mentioned above, it is a fair solution. *UTV Software Communications* v. *1337X.To*[76] is a matter which was filed in the High Court of Delhi whereby the plaintiffs have prayed for blocking websites which contain content violating Plaintiffs' copyright. The Plaintiffs have sought for a dynamic injunction in this case. The matter is still pending before the court.

Therefore, it is the need of the hour to develop a mechanism for grant of dynamic injunctions, in order to have a simple solution for techno-legal complexities. We would conclude by saying that the need of the hour is for judicial dynamism in India to work its way again and mould the remedy of injunction to now implement a 'dynamic injunction – injunction 2.0'.

[76] 2019(78) PTC375(Del). (The decision in this case was reserved and has been pronounced after this article was written by us. We will address the decision in a follow up article, *available at*: http://lobis.nic.in/ddir/dhc/MMH/judgement/11-04-2019/MMH10042019SC7242017.pdf