INDUSLAW
THOUGHT LEADERSHIP ... APPLIED

DETAILS OF INFRINGERS CANNOT BE MASKED UNDER THE GARB OF PRIVACY FEATURES, RULES HIGH COURT OF DELHI

Authors: Bharadwaj Jaishankar, Kshitij Parashar

INTRODUCTION

The rise of internet throughout the world has also caused a rapid increase in cyber-crimes such as piracy, sale of counterfeit products, identity fraud etc. Courts in India are taking steps to deal with such issues in cases involving copyright infringement, misuse of registered trademarks/ names/brands by fake/rogue websites impersonating as the real one and deceiving customers. Recently, the Hon'ble High Court of Delhi ("**High Court**") in several cases has granted interim injunctions against several fake/ rogue websites, involved in selling counterfeit products or circulating copyrighted content illegally. A peculiar aspect in all these cases has been that the High Court has delved into the issue of the failure of various Domain Name Registrar ("**DNRs**") and instant messaging platforms from complying with the Court's orders and provisions of the Information Technology Act, 2000 ("**IT Act**"). These DNRs and messaging platforms have been directed by the Court to disclose details of entities/persons uploading infringing material on their platforms.

PRACTICAL DIFFICULTIES VIS À VIS CYBER CRIMES

Jurisdiction

The primary issue faced by Indian Courts while adjudicating cases involving infringement through cyber space is whether they have jurisdiction over online platforms (mobile messaging applications, DNRs, social media platforms etc.) which are located abroad or have servers outside the territory of India. The High Court in the case of *Neetu Singh & Anr. v. Telegram FZ LLC & Ors.*[1]("**Neetu Singh's case**") directly dealt with this issue. In this case, the Plaintiff's copyrighted material such as books and video lectures were being illegally circulated on various Telegram groups. Telegram challenged the jurisdiction of the High Court on the ground that its servers are located in Singapore and thus, outside the Court's jurisdiction.

The High Court dismissed this plea of Telegram. It stated that courts in India have the natural forum of jurisdiction in such disputes as the infringement is unabashedly continuing in India. Further, the copyrighted material is related to Indian examination/study materials the source of the infringing channels would be in India, the accounts of such infringing channels would have been created from India and the data of such accounts would have been uploaded from India.

Privacy protect feature

In *Dabur India Limited v. Ashok Kumar and Ors.*[2] ("**Dabur's case**"), the High Court clubbed several suits filed by multiple brand owners, seeking reliefs against the misuse of their marks/names/brands by unauthorized persons, who registered such marks as part of their domain names. The major grievance of the Plaintiffs was the ability of such domain name registrants to conceal their identity by availing services like privacy protect and proxy domain provided by DNRs. The High Court noted that the proliferation in such domain names has resulted in an enormous damage to public, who have been misled to believe that such impostor domain names belong to the actual brand owners.

Further, it noted practical issues faced by the aggrieved parties in such cases - : (i) in cases involving fake/rogue websites, inability of the plaintiff to serve those DNRs, who do not have office(s) in India; or (ii) failure in the implementation of the orders passed against DNRs; and (iii) obtaining data relating to the registrants of the domain names from respective DNRs.

While resolving these issues, the High Court relied upon Rule 3(2) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("**IT Rules, 2021**"). This Rule requires the DNRs to appoint grievance officers and provide their name, designation, contact address and number etc. so that the public can address their grievances to them and to also ensure implementation of Court orders. However, just like *Neetu Singh's case* the issue of want of jurisdiction of the High Court was again argued by the DNRs.

The High Court drew a negative inference towards the privacy protect feature offered by the DNRs. This is because even after DNR block the fake/rogue website, the infringers are still capable of finding a new way (via a new website/private channel) to circulate the infringing content. Accordingly, the Court observed that this feature is increasingly resorted to by such infringers. Thus, there is a need to disable privacy features such that the details of the registrant are visible on 'who.is' and other databases. Additionally, the High Court laid emphasis on abiding with Section 79(3)(b) of the Information Technology Act, 2000 by intermediaries (including DNRs and messaging platforms) which mandates intermediaries to expeditiously remove or disable access to unlawful material.

The argument posed by the DNRs in support of privacy protect features, for the sole purpose of commercial interest, is to guarantee and protect the right to privacy of registrants. However, while relying on the judgment in *Justice K.S. Puttaswamy v. Union of India & Ors.*[3], the High Court observed that intermediaries cannot argue the right to privacy when the disclosure of the information is permissible by law and is directly proportional to the nature of encroachment. Moreover, when it comes to rights of the public in general, the provisions of IT Act are supplementary to the provisions of Copyright Act as stated under Section 81 of the IT Act.[4]

Thus, the High Court in *Dabur's case*, while ensuring public interest over commercial interest, ordered the respective DNRs to file an affidavit disclosing the details of the registrants along with their complete contact details, postal address, email address, bank account details, and telephone numbers, etc.[5]

Whereas, in *Neetu Singh's case*, Telegram was directed to disclose the identity of the person registering the channel/messaging groups and details like IP addresses, mobile numbers and devices used for operating channels/ messaging groups in a sealed cover.

1. 2022 SCC OnLine Del 2637, judgment dated August 30, 2022.
2. CS (COMM) 135/2022, orders dated 03.08.2022, 13.09.2022 and 14.09.2022.
3. (2017) 10 SCC 1.
4. *Christian Louboutin Sas v. Nakul Bajaj & Ors.* (2018) 253 DLT 728.
5. Ibid at 2.

A similar view has been taken by the High Court in *Star India Private Ltd. & Anr. v. MHDTV World & Ors.* ('**Star Case**')[6]. In this case, the Plaintiff had filed a suit seeking an injunction to restrain the illegal and unauthorized dissemination of the Asia Cup Cricket matches and associated content therewith, by the Defendants. While granting an injunction in favor of the Plaintiff, the High Court directed the relevant DNRs to *inter alia* disclose: (i) complete details (name, address, email address, phone number, IP address etc.) of the registrants of rogue websites/domain names impleaded as Defendants; (ii) mode of payment along with payment details used for registration of rogue websites/domain name by the respective registrants.

However, as per High Court's own observation in *Dabur's case*, even after directing the DNRs to submit the details of the registrant of the domain names, the information collected by the DNRs at the registration stage is insufficient, fictitious, or untraceable. Due to such complications, tracing owners required multiple court orders and police investigations. In *Dabur's case*, the High Court has directed the stakeholders such as the DNRs, Delhi Police, Ministry of Electronics and Information Technology, Department of Telecommunication, National Internet Exchange of India to discuss and provide recommendations to resolve the issues. In the cases involving financial fraud, the High Court has also directed an Investigating Officer of the Delhi Police to file the status report of the investigation in such cases. Recently, the High Court has also looped in the Reserve Bank of India, since several Plaintiffs had complained that bank account details of the Defendants/persons impersonating the Plaintiffs are incorrect and the names under which bank accounts have been opened are fictitious. The Plaintiffs also complained that banks are not placing on record - the bank statements of the accounts complained of and the KYC details of such bank account holders. The High Court directed the RBI to consider the issue of providing incorrect details for opening bank accounts. Further, the banks have been directed to provide the KYC details and bank account statements of the Defendants, as and when requested.[7]

6. 2022 SCC OnLine Del 3770.
7. Order dated 01.12.2022 in *Dabur's case*.

CONCLUSION & THE WAY FORWARD

The key takeaway from the High Court's orders is that on a digital platform, the relevant registrants, be it the DNRs or the mobile application, are bound to disclose the identity of the infringer. The infringer cannot be provided a safe haven under the garb of anonymity. While all these matters are primarily IP infringement cases, the High Court has broadened the scope of the cases to deal with the issue of non-disclosure of details of the infringer on an online platform. The internet provides a quick access to any information/services required but it also provides anonymity to infringers who seek to hide their identity. The observations of the High Court in the cases discussed in this article has exposed the loopholes in the IT laws. However, the Courts have been taking steps in the right direction by filling the gaps in the law.

INDUSLAW
THOUGHT LEADERSHIP ... APPLIED

www.induslaw.com

OUR OFFICES

BENGALURU
101, 1st Floor, "Embassy Classic"# 11
Vittal Mallya Road
Bengaluru 560 001
T: +91 80 4072 6600
F: +91 80 4072 6666
E: bangalore@induslaw.com

DELHI
2nd Floor, Block D
The MIRA, Mathura Road, Ishwar Nagar
New Delhi 110 065
T: +91 11 4782 1000
F: +91 11 4782 1097
E: delhi@induslaw.com

HYDERABAD
204, Ashoka Capitol, Road No. 2
Banjarahills
Hyderabad 500 034
T: +91 40 4026 4624
F: +91 40 4004 0979
E: hyderabad@induslaw.com

MUMBAI
1502B, 15th Floor
Tower – 1C, One Indiabulls Centre
Senapati Bapat Marg, Lower Parel
Mumbai – 400013
T: +91 22 4920 7200
F: +91 22 4920 7299
E: mumbai@induslaw.com

CHENNAI
#11, Venkatraman Street, T Nagar,
Chennai - 600017 India
T: +91 44 4354 6600
F: +91 44 4354 6600
E: chennai@induslaw.com