Intermediary liabilities and safe harbour – an umbrella for the rain?

Thought Leadership • July 19, 2022

By Safir Anand *Anand and Anand senior partner Safir Anand explains why regulating intermediary platforms is essential to prevent content misuse.* Intermediaries act as essential cogs in the wheel of exercising the right to freedom of speech, expression and content delivery across jurisdictions. However, given the flow of inexhaustible data, intermediaries are often held vicariously accountable for unlawful and unscrupulous content posted by users on their platforms. In an information technology law context, the concept of intermediary liability is often deeply analysed and debated. In most democratic countries, three common approaches generally apply to guide the discussion.

1. *An awareness or actual knowledge approach* requires that the intermediaries be held responsible for any unlawful content or activity only if they are aware or have "actual knowledge" of content missue and when alerted, would have to take swift action to remove it. However, the approach incentivizes platforms to take down more content than may be necessary, retaliate against content they oppose by falsely reporting it, or imposing significant moderation costs on platforms by forcing them to review content.
2. *A notice and takedown approach is* where an individual submits a Notice of Complaint that identifies specific harmful or illegal content. The website hosting the content must contact the author of the content or, if the author's identity is unknown, remove the content. The author can then file a counter-notice either consenting or refusing to the content's removal. The drawback of this approach, however, is that it incentivizes online services to remove content which is controversial but which may not be harmful or illegal, thereby jeopardizing the Internet's role as a forum for free and open discourse when platforms remove legitimate content.
3. *A mere conduit, caching and hosting approach* is most commonly followed in the European Union where the e-Commerce Directive extends liability protections to online services up to the extent their activity "is of a mere technical, automatic and passive nature." The liability protections extend only to "passive" online services offering "mere conduit" (Article 12), "caching" (Article 13), or "hosting" (Article 14) services. Thus, with no active involvement, the Intermediaries remain protected.

The European Union's intermediary liability regime In the European Union, liability of Internet Intermediaries for third parties' content has been regulated by the e-Commerce Directive. Until 2019, the government's policy remained as stated. In October 2020, the government commented that it, "has no current plans to change the UK's intermediary liability regime or its approach to prohibition on general monitoring requirements". As noted, Articles 12 to 14 provide limitations on the Liability of Conduits, Caches and Hosts for unlawful user information. Article 15 prohibits EU member states from imposing general monitoring obligations on those intermediaries. *India's intermediary liability regime*

India's Information Technology Act, 2000 (IT Act, 2000) establishes the concept of "safe harbour" as immunization to intermediaries. Under the same act, provisions for intermediary liability immunization first came through an amendment to the IT Act in 2000 (through amendment of Section 79), which exempts Intermediaries from any liability for any third-party content made available on its platform read with Rule 3 of the Information Technology (Intermediaries Guidelines) Rules, 2011 ("IT Rules"). Before this, it was upon the Intermediary to seek any protection subject to proving an offence / contravention committed without their actual knowledge along with undertaking due diligence. Section 79(1) of the IT Act provides Intermediaries immunity with respect to any third-party content, data or information hosted by them. This is limited by section 79(2) and (3) of the IT Act, which prescribes that this immunity is applicable only when an Intermediary's role is passive and technical in nature, and provides that an Intermediary cannot claim immunity if it has *"...conspired or abetted or aided or induced...in the commission of the unlawful act"*. Section 79(3)(b) provides for a 'notice and take down' regime, wherein an intermediary is required to take down infringing content upon receiving actual knowledge of its existence. Further, IT Rule 3 provides that an intermediary shall observe due diligence, which will absolve them of liability for third-party content. Such due diligence includes publishing its Rules and Regulations (including user agreement and privacy policy), which shall inform users to not upload any information which is misleading/fake and infringes trademark, patent copyright or any other proprietary rights. Subsequently, various judicial enactments establishing actual knowledge were enforced in cases including in *Shreya Singhal v. Union of India* [2015 (5) SCC 1], and *Myspace Inc v. Super Cassettes Limited* [2017 (69) PTC 1 (Del)]. In 2018, the Delhi High Court in the landmark case of *Christian Louboutin v. Nakul Bajaj [CS (COMM) 344/2018]*, differentiated between e-commerce platforms which act just as an "Intermediary" and those which act as an "active agent" in selling goods. To that extent, the court noted certain criterion to identify the role of e-commerce platforms relating to transportation, quality assurance, collection of payment, reviews, authenticity guarantee, advertisement/promotion of the product, membership, providing specific discounts to members, uploading the entry of product, booking ad-space, deep-linking to the trademark's owner website, etc. The Delhi High Court observed that *"...the so-called safe harbour provisions for Intermediaries are meant for promoting genuine businesses which are inactive Intermediaries, and not to harass Intermediaries in any way, the obligation to observe due diligence, coupled with the Intermediary guidelines which provides specifically that such due diligence also requires that the information which is hosted does not violate IP rights, shows that e-commerce platforms which actively conspire, abet or aide, or induce commission of unlawful acts on their website cannot go scot free"*. The criteria laid down in this case was also followed in subsequent cases by the Delhi High Court. Along the same lines, the Delhi High Court in *Amazon Seller Services Pvt. Ltd. vs Modicare Ltd. & Ors.* [FAO(OS) 540/2011] further strengthened the safe harbour provided to e-commerce intermediaries by ruling that *"...the value-added services provided by them as online market places...do not dilute the safe harbour granted to them under Section 79 of the IT Act. Section 2 (1) (w) of the IT Act does envisage that such intermediaries could provide value-added services to third party sellers." Impact of recent*

developments Post-Brexit in the United Kingdom, the Online Harms proposal was introduced in the Parliament, originally in 2019, to tackle the access of harmful content online. The proposal adopts the idea of "the systematic duty of care" model, i.e. measures that platforms should impose for reducing online harms, which also provides the regulator OFCOM the power to fine firms or block access to sites that fail to comply with the new rules. In this proposal was a detectable drift into proposing proactive monitoring obligations that could not readily be reconciled with that earlier policy of mere passive participation. A new version of its post-Brexit e-Commerce Directive guidance, published on 18 January 2021 stated: *".....for companies that host user-generated content on their online services, there will continue to be a 'notice and take down' regime where the platform must remove illegal content that they become aware of or risk incurring liability. The concept combines generally reducing the risk of harms with improved notice and takedown measures as well as introducing new monitoring obligations"*. This could entail measures by platforms such as to deploy automated filters to find duplicates of unlawful material, instruct employees to search for terms associated with illegal activity and take down suspicious results, or periodically review posts in forums with a history of illegality. The impact of this would be that it will lead to a lot of matters being brought to court as well as question the platform user's fundamental rights to freedom of speech and expression. Thus, although a commitment to preserving some kind of hosting protection remains, there is now silence on preserving the prohibition on general monitoring obligations. This could interfere majorly with the intermediaries general passive approach, freedom to conduct its reasonable duty of care as well as erosion of the Articles 12 to 14 due to the statute being amended over time. Also, related are the Recent Amendments to the European Union's Digital Markets Act (DMA) being finalized in EU, and aimed at regulating the giant Intermediary platforms (also referred to as "gatekeepers") are being touted as bringing in a "new era of tech regulation" worldwide. The amendments to the DMA require the large digital platform companies to adhere to a long list of obligations and prohibitions, forcing many of them to significantly change the way they interact with consumers, business partners and competitors. The amendments aim to allow fair competition and make them more approachable to customers by offering them a choice to use the core services of the giant intermediary platforms such as browsers, search engines or messaging, without losing control over their data. The amendments include provisions for the larger messaging services to open up and interoperate with smaller messaging platforms, and if they so request, to allow interoperability by customers to exchange messages, send files or make video calls across messaging apps, thus giving them more choice. Further, the amendments allow for use of personal data for advertising target audiences only with explicit consent of these intermediary platforms, along with allowing them freedom to search with their preferred browser, virtual assistants and search engines. Though the imposition of sanctions make it incumbent on the intermediaries to follow the rules or face hefty fines extending from 10% of their total worldwide turnover in the preceding financial year, and 20% in case of repeated infringements, including a ban in case of systematic infringements, the DMA places obligations only on "gatekeepers," which are companies that create bottlenecks between businesses and consumers and have an entrenched position in digital markets. The companies will be hit by the rules only if:

- They have an annual turnover of €7.5 billion within the EU or a worldwide market valuation of €75 billion;
- Gatekeepers must also have at least 45 million monthly individual end-users and 100,000 business users; and
- Gatekeepers must control one or more "core platform services" such as "marketplaces and app stores, search engines, social networking, cloud services, advertising services, voice assistants and web browsers." In practice, this will almost certainly include Meta (Facebook), Apple, Alphabet (Google), Amazon, and possibly a few others.

How these amendments will be able to create a level playing field between businesses is yet to be seen, and the restrictions and sanctions appear to be quite stringent. Yet, he positive side is that these may create an effective competition policy for the internet, one that keeps users' needs front and center, and will help align market forces and innovation to serve users' security and privacy needs. With respect to India, it appears that it too has followed suit to the UK's new monitoring regime for intermediaries by enacting the new Intermediary Liability and Digital Media Regulations (The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 were notified by the Central Government on 25th February 2021) which, by expanding the scope of due diligence obligations, is set to harm the open internet including the users and might have an devastating impact on freedom of expression, privacy and security. The due diligence requirements entail publishing of details, disabling access, preserving information, removal of explicit content, furnishing information or assistance to government agency, providing for a grievance re-dressal mechanism, and many other such policing measures. Further developments in this field pertain to the recent judgements of the Delhi High Court, *(M/s DRS Logistics Private Limited & Others v Google India Pvt Ltd & Others and MakeMyTrip India Private Limited vs Booking.Com B. V & Ors.)* which say that the use of registered trademarks as keywords on Google Ads by a competitor, would amount to trademark infringement. The judgments also shed light on the liability of intermediaries in investigating the use of registered trademarks on its platform and preventing misuse and infringement. In the case of DRS Logistics, the defendants argued that, the mere use of the mark as a keyword that acts as a back-end trigger does not amount to the use of the trademark. However, the Court reiterated that the advertisements triggered by a third party will lead to confusion regarding the origin of the goods and services advertised. Further, the court issued directions which included that:

- Google shall investigate any complaint made by the plaintiffs alleging infringement causing a diversion of web traffic from the plaintiffs' website;
- Google shall investigate and review the overall effect of an ad to ascertain that the same is not infringing/passing off the trademark of the plaintiffs; and
- If it is found that the usage of the trademarks and its variation as keywords and/or overall effect of the ad has the effect of infringing/passing off the trademark of the plaintiffs, then Google shall restrain the advertiser from using the same and remove/block such advertisements.

The Delhi High Court in this case has set an important precedent as the directions of the court ordering Google to investigate the infringement complaints or take suo moto action created a direct liability upon the big giant platform (intermediary) to prevent infringement of trademarks; further the directions issued will keep Google and the advertisers in check to avoid infringing on another party's rights. Additionally, the court had decided on infringement caused by the invisible use of trademarks as keywords especially when there is no provision of the Act dealing with such use. In this case, the court has directly held Google liable for its actions through the Ads Program, as it has enabled competitors to free-ride on the reputation and goodwill of trademark owners. In her interim order in the MakeMyTrip case, Justice Pratibha Singh ruled that that the use of the 'MakeMyTrip' mark as a keyword in the Google Ads programme by Booking.com and Google would amount to trademark infringement and be detrimental to the plaintiff's (MakeMyTrip) monetary interest and brand equity. Additionally the order conferred that in the European Union, due to the monitoring regulations, Google being an intermediary would investigate the use of trademarks as keywords in published ads. In India, there is no such requirement imposed on the intermediary platforms. The Alliance of Digital India Foundation (ADIF) hailed the High Court order and stated that "It is unethical of Google to encash upon the goodwill and reputation of brands by allowing their competitors to use their registered trademarks as keywords in Google Ads." *Boon or bane for intermediaries?* These judgments herald a new era for intermediaries' liability in India and the European Union, with new, more stringent monitoring regulations in place in both jurisdictions. At the same time, it is important to note that the concept of intermediary liability is still evolving and growing. In this context, there needs to be a balance between granting exemptions and imposing liabilities. This is not so easy a task. On one hand, the intermediaries, which are limited with technical role, should not be obliged to monitor or investigate any content that they store or provide access to. However the other side is that because they have such a highly technical role, they are the entities that are perfectly capable of controlling and avoiding any illegal content. Regulation of the intermediary platforms is essential to ensure no misuse with regard to content is possible, which in a way can made possible only by imposing stringent regulatory provisions on the intermediaries. Therefore, the idea of prior positive obligation on the part of intermediary to reduce risks arising from third party content without burdening it to undertake all measures to ensure safety should be sought, with some stringent monitoring regulations which do not adversely impact the independence of intermediaries and harm users. A regime is required wherein the intermediaries can still operate in line with broad understandings of freedom of speech but also would cooperate, in a way that can be expected within the boundary of their duties, and even be held liable from any infringing content that they host or provide access. This article was originally published on Luxury Law Alliance

KEY CONTACT

Safir Anand

Senior Partner

View Bio of Safir Anand