Shielding internet intermediaries from copyright liability–A comparative discourse on safe harbours in Singapore and India*

Althaf Marsoof
Assistant Professor of Law, Nanyang Business School, Singapore

Indranath Gupta
Professor of Law, Jindal Global Law School, India

Biographies

Dr Althaf Marsoof
Althaf Marsoof is an Assistant Professor of Law at the Nanyang Business School (NBS), Nanyang Technological University, Singapore. Prior to joining the NBS, he spent three years at the Dickson Poon School of Law at King's College London, where he completed his Doctoral research investigating approaches to, and challenges in, holding internet intermediaries accountable for infringements of trademark rights. His research was fully funded by the Dickson Poon PhD Scholarship grant. Prior to moving into full-time academia, he worked for over six years as a State Counsel attached to the Attorney General's Department in Sri Lanka. He holds a Bachelor of Science in the field of information technology from the Curtin University (Australia) and a Master of Laws (with first class honours) from the University of Cambridge, UK. He spent a year in Australia researching on the applicability of Australian laws relating to trademarks and consumer protection, as well as common law tort principles, to the context of trademark infringements committed in the online environment. This research was the basis for his MPhil thesis at the University of Queensland, which was supported by two grants: the International Postgraduate Research and Centennial scholarships.

Dr Indranath Gupta
Indranath Gupta is a Professor of Law and Controller of Examinations at the Jindal Global Law School (JGLS), India. He is an Assistant Director of the Centre for Postgraduate Legal Studies and the Centre for Intellectual Property and Technology Law. He is the Co-Director of JIRICO, Assistant Dean (Student Initiatives) and Senior Fellow at the Jindal Institute of Behavioural Sciences (JIBS). He received his LL.B. degree from the University of Calcutta, India; holds an LL.M. with distinction from the University of Aberdeen, UK; and holds a postgraduate research LL.M. in Computer Law from the University of East Anglia, UK. He obtained his Ph.D. from Brunel University, London, UK. He has been involved in qualitative and quantitative research. He was appointed as the research collaborator by the Università Bocconi, Milan, Italy, for a project funded by the European Commission under the 7th Framework Programme. He has also worked as an advocate in a solicitor's firm at the Calcutta High Court. He has published in European and Indian Law journals and has spoken at international conferences and seminars. His research areas include database right, copyright, data protection, cyber law and the interface of IP and competition law.

* The authors acknowledge the research assistance provided by Mr Deepesh Jain, who, at the time, was a research assistant attached to the JGLS. This paper is an outcome of a research project that was funded by the first author's start-up research grant.

Shielding internet intermediaries from copyright liability–A comparative discourse on safe harbours in Singapore and India

Abstract

Without intermediaries that provide access to, host and link content, the internet will not be the vibrant place it is today. Yet with the rising number of online copyright infringements, right holders have increasingly shifted their focus to intermediaries in their efforts to curb infringements. This has led to internet intermediaries being increasingly exposed to copyright liability. In light of this, safe harbours that provide certain classes of intermediaries with conditional immunity play an important role in maintaining a healthy balance between the interests of right holders and third parties. In the copyright context, the Digital Millennium Copyright Act 1998 (DMCA) enacted in the United States was the first instance where such a safe harbour was afforded to internet intermediaries. During the two decades of the DMCA's operation, it has been used as a blueprint to shape safe harbours in other jurisdictions. This article focusses on two such jurisdictions–namely, Singapore and India. This article provides a comparative and in-depth analysis of the safe harbour frameworks in the two jurisdictions, while mapping out how they compare with the DMCA. In the process, the article highlights a number of features in the DMCA that have been remodelled in Singapore and India.

Introduction

The internet comprises many intermediaries that facilitate access to, store and link content–Internet Service Providers (ISPs), hosts and search engines playing a crucial role in this regard. Without intermediaries, the internet will not be the thriving place it is today. This is precisely why it is necessary to ensure that intermediaries are provided sufficient protection from liability for unlawful content generated by those who make use of the internet. In the copyright context, the Digital Millennium Copyright Act 1998 (DMCA)[1] enacted in the United States (US) for the first time introduced a safe harbour for intermediaries that shielded them from copyright liability upon fulfilling certain conditions. The DMCA has provided the blueprint, and impetus, for similar safe harbours in other jurisdictions. The focus of this article is on two such jurisdictions–namely, Singapore and India.

In view of the comparative nature of the article, it begins by providing some background and context to the DMCA, followed by a discussion on the key features of the US's safe harbour. In the second part, the article provides an in-depth and comprehensive analysis of the safe harbours adopted in Singapore and India, the features of which are mapped against the DMCA safe harbour in order to highlight how the DMCA has been remodelled in those jurisdictions. The strengths and weaknesses of the Singaporean and Indian approaches are also considered in the process.

The Digital Millennium Copyright Act

Some background and context

The enactment of section 512 of the DMCA in 1998, commonly referred to as the DMCA safe harbour or simply DMCA 512, could be regarded as a significant milestone in US copyright history. Before the DMCA was enacted, courts in the US had adopted a very aggressive approach towards intermediaries that operated in the internet environment by finding direct copyright liability. The bulletin board cases that came up in the first half of the 1990s amply illustrate this trend. It appears that bulletin boards were the first forums the internet saw, allowing users to upload, share and download content. They were intermediaries that provided a platform where users could store data and content, in many ways resembling the modern-day host.

One of the earliest cases to be filed against a bulletin board was *Playboy v Frena* (1993), which came up before the US District Court (Middle District of Florida). In that case, the complaint of Playboy Enterprises Inc (PEI) was that a bulletin board, operated by the defendant (i.e. Frena) distributed unauthorised copies of PEI's copyrighted photographs. According to the evidence, 170 of the images on the bulletin board were copies of photographs taken from PEI's copyrighted material. Frena in his defence admitted that these images were displayed on the bulletin board, he never obtained any authorisation from PEI in respect of the images and that the images were substantially similar to the copyrighted PEI photographs. It was also admitted that the images available on the bulletin board had been downloaded by the users of the service. However, and perhaps importantly, Frena took up the position that he never uploaded any of the images in which PEI had copyright and that it was the subscribers to the bulletin board that had uploaded the contentious photographs. Frena also pleaded that as soon as he was served with a summons and was made aware of the infringements, he removed the infringing images from the bulletin board and since then monitored the service in order to prevent further infringing images from being uploaded by users.

The right in question was PEI's right to distribute copies of, and display, the copyrighted work to the public, which were exclusive rights vested under the US Copyright Act 1976 (17 U.S.C. §106) on a copyright owner. The Court held that "[t]here is no dispute that […] Frena supplied a product containing unauthorized copies of a copyrighted work. It does not matter that […] Frena claims he did not make the copies" and that the defendant's "display of PEI's copyrighted photographs to subscribers was a public display" (*Playboy v Frena*, 1993, pp.1556-57) Thus, although Frena was merely providing the services of a bulletin board, that permitted third parties to upload images onto the platform, thus, enabling the public display and distribution of those images, he was caught up for *direct* copyright infringement. It was not a defence for Frena that he lacked knowledge of the infringements or that he took prompt action once he did become aware. Thus, even though Frena through his bulletin board was acting as an intermediary–providing only the technical functions of a host that facilitated subscribers to upload, distribute and display content (images)–the Court felt it fit to find Frena and his bulletin board liable for copyright infringement on the basis that they were primary infringers.

The second instance where direct copyright infringement was found on the part of bulletin board was in *Sega Enterprises Ltd v Maphia* (*Sega v Maphia*), albeit this was in the context of a hearing for a preliminary injunction. This case concerned a bulletin board known as 'Maphia' operated by Sherman. The bulletin board was dedicated to sharing video games. Just as in

Playboy v Frena (1993), the users of the bulletin board uploaded and downloaded the games in which Sega had copyright. This privilege was afforded to anyone who subscribed to the bulletin board's service or to those who had purchased a device from Maphia that enabled Sega game cartridges to be copied and distributed via the bulletin board with other users. It is quite clear that Maphia's business model was geared to promote the infringement of Sega's copyright. While this no doubt was a suitable case to find Maphia, and its operator, liable for copyright infringement, what was troubling is the basis upon which the US District Court (Northern District of California) imputed liability on the intermediary concerned–"Sega has established a *prima facie* case of *direct copyright infringement*" (*Sega v Maphia*, p.686).

The fact that US courts in, at least, two instances had found an intermediary that did not itself commit infringements liable for *direct* copyright infringement was troubling and destined to have ramifications on other intermediaries providing similar hosting services. Notably, however, these decisions were doubted in *RTC v Netcom* (1995), which not surprisingly also concerned a bulletin board, as well as an ISP. The facts in this case were similar to those of the previous cases–in that certain copyrighted material became published and available on an online forum. Apart from the person who uploaded the infringing material (Dennis Erlich) onto the forum, a bulletin board and an ISP were also made defendants. As such, the Court had to consider the liability of actors who provided the technical facilities used by Dennis Erlich in uploading the infringing material onto the forum. Commenting on *Playboy v Frena* (1993), the US District Court (Northern District of California) in *RTC v Netcom* (1995) Court observed:

> "*Playboy* concluded that the defendant infringed the plaintiff's exclusive rights to publicly distribute and display copies of its works. […] The court is not entirely convinced that the mere possession of a digital copy on a [Bulletin Board] that is accessible to some members of the public constitutes direct infringement by the [Bulletin Board] operator" (*RTC v Netcom*, 1995, para 21).

Commenting on *Sega v Maphia*, the same Court observed:

> "This court is not convinced that *Sega* provides support for a finding of direct infringement where copies are made on a defendant's [Bulletin Board] by users who upload files. Although there is some language in *Sega* regarding direct infringement, it is entirely conclusory. […] The court's reference to the "knowledge of Defendant" indicates that the court was focusing on contributory infringement, as knowledge is not an element of direct infringement" (*RTC v Netcom*, 1995, para 19).

Accordingly, in *RTC v Netcom* (1995), the Court decided that the better approach to dealing with the liability of intermediaries was to treat them as contributory infringers: "Netcom is not free from liability just because it did not directly infringe plaintiffs' works; it may still be liable as a contributory infringer" (*RTC v Netcom*, 1995, para 24). The decision in *RTC v Netcom* (1995) was followed by the US District Court (Northern District of Illinois) in *Marobie-FL v NAFED* (1997). Interestingly, Wilken J, who awarded the preliminary injunction against Maphia in *Sega v Maphia* (1994), on the basis that Maphia had engaged in direct copyright infringement, seems to have been influenced by the decision in *RTC v Netcom* (1995) by the time he had to make the final award in that case.[2] Thus, the judge found that Maphia did not attract *direct* copyright liability,[3] but only contributory liability.[4]

Given that US courts were adopting contradictory approaches as regards the liability of intermediaries, although it seems that the general trend was an expansion of the reach of copyright liability, particularly through the vessel of contributory infringement, to include new intermediaries in an environment that was emerging very fast. This led to a debate on how the liability of online actors should be handled, as intermediaries, in particular, were crucial to the development of the internet. Bartholomew & Tehranian (2006, p.1407) have suggested that "the courts' willingness to expand the reach of contributory […] liability in copyright law has led to congressional involvement to *limit* secondary liability." Outside the sphere of intellectual property law, intermediaries that operated on the internet became completely immune from civil liability for content that originated from third party users. This was consequent to the enactment of the Communications Decency Act 1996 (CDA), which provided in section 230 that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider" (47 U.S.C. §230(c)(1)). While section 230 has been described as the 'saviour of free speech' (Ardia, 2010), section 230(c)(3) made it explicitly clear that nothing in section 230 applied "to limit or expand any law pertaining to intellectual property" (47 U.S.C. §230(e)(2)). As such, the enactment of the CDA did not address the concerns of intermediaries as regards their liability under copyright law.

There was, and still will be, opposition against limiting the liability of internet intermediaries. For instance, in the context of section 230 of the CDA, Holland (2010, p.199) has been suggested that the legislative provision "has created an environment in which many of the norms and regulatory mechanisms present in the offline world are effectively inapplicable [to the online context]. This is so not because the very nature of cyberspace makes such application impossible, or because sovereign law is necessarily ineffective or invalid, but rather because sovereign law has affirmatively created that condition." More specifically, in the copyright context, the Information Infrastructure Task Force (IITS), established by the Clinton administration, through its Working Group on Intellectual Property observed in a report:

> On-line service providers currently provide a number of services. With respect to the allowance of uploading of material by their subscribers, they are, in essence, acting as an electronic publisher. In other instances, they perform other functions. No one rule may be appropriate. If an entity provided only the wires and conduits -- such as the telephone company, it would have a good argument for an exemption if it was truly in the same position as a common carrier and could not control who or what was on its system. The same could be true for an on-line service provider who unknowingly transmitted encrypted infringing material. It would be unfair -- and set a dangerous precedent -- to allow one class of distributors to self-determine their liability by refusing to take responsibility. This would encourage intentional and willful ignorance. Whether or not they choose to reserve the right to control activities on their systems, they have that right. Service providers expect compensation for the use of their facilities -- and the works thereon -- and have the ability to disconnect subscribers who take their services without payment. They have the same ability with respect to subscribers who break the law (Information Infrastructure Task Force, 1995).

What may be gleaned from the above is that the IITS opposed the granting of complete immunity to intermediaries, whereas they have suggested that intermediaries (unless they are mere conduits) should take responsibility for content that is published and transmitted on their

networks. It was in this backdrop that the US Congress decided to enact section 512 of the DMCA, which to a great extent is consistent with IITS's position. Thus, under this provision, although intermediaries are not completely immune from copyright liability, they are conferred conditional immunity upon the fulfilment of certain requirements as set out therein aimed at protecting the interests of copyright owners. At the time the DMCA was enacted, it was seen as a worthy compromise that balanced the interests of copyright owners and internet subscribers that generate and share content. More importantly, as the Senate Report on the DMCA illustrates, the DMCA was regarded as a crucial legislative intervention to preserve innovations on the internet:

> At the same time, without clarification of their liability, service providers may hesitate to make the necessary investment in the expansion of the speed and capacity of the Internet. […] In short, by limiting the liability of service providers, the DMCA ensures that the efficiency of the Internet will continue to improve and that the variety and quality of services on the Internet will continue to expand (Senate Report, 1998, p.8).

Apart from being an influence in the home-front, the DMCA has been very influential in shaping copyright law and policy in other parts of the world. In some instances, this has been due to DMCA-*like* standards being incorporated into free trade agreements between the US and other nations. Singapore provides a typical example of this. Whereas in other instances safe harbours from the West–mainly the DMCA 512, but also to some extent the safe harbour applicable in the European Union (EU) as incorporated into the E-Commerce Directive[5]–have influenced how domestic law in other jurisdictions is shaped–India providing an example of this. However, before dealing with how the DMCA safe harbour has influenced legislation in Singapore and India, it is useful to set out the key features of the safe harbour, as well as the case law and academic commentaries that have analysed those features.

The DMCA safe harbour and the practice of notice and takedown

The DMCA safe harbour applies to any 'service provider', as defined in section 512(k)(1), that is engaged in any one or more of the four categories of activities that are identified in sections 512(a) to (d)–i.e. transitory digital network communications,[6] system caching,[7] hosting[8] and information location.[9] The term 'service provider' attracts a dual definition. Section 512(k)(1)(A) provides that for the purposes of section 512(a)–i.e. transitory digital network communications–a service provider is "an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received." This definition fits the description of typical ISPs that provide access to the internet. Whereas, section 512(k)(1)(B) defines 'service provider' for the purposes of sections 512(b), (c) and (d) as "a provider of online services or network access, or the operator of facilities therefor, and includes an entity described in subparagraph (A)." The latter definition is seemingly much broader as it includes a provider of online services, which includes entities that engage in system caching, hosting and information location, as well as internet access. In *Viacom v YouTube* (2012), the US Court of Appeals (2nd Cir) observed in respect of the activities of YouTube, which clearly comes within activities described in section 512(d) of the DMCA, that:

> "Most notably, [the DMCA] contains two definitions of "service provider." […] The narrower definition, which applies only to service providers falling under § 512(a),

is limited to entities that "offer[ ] the transmission, routing or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received." […] No such limitation appears in the broader definition, which applies to service providers—including YouTube—falling under § 512(c)" (para 76).

In *Corbis v Amazon* (2004), the US District Court (Western District of Washington) had to consider whether Amazon could be regarded as a 'service provider' under section 512(k)(1)(B) and decided that "[t]his definition encompasses a broad variety of Internet activities […] and there is no doubt that Amazon fits within the definition" (at p.1100).[10]

Once an intermediary fits the description of a 'service provider', the applicability of the DMCA safe harbour depends on whether it satisfies the conditions set out therein. These conditions vary depending on the nature of activities carried out by the service provider. There is, however, one condition that applies across the board to all categories of activities and service providers– that is, for the safe harbour to apply, service providers must adopt and reasonably implement a repeat infringer policy and ensure that they adopt and do not interfere with standard technical measures.[11]

Section 512(a) applies to 'transitory digital network communications'. Thus, service providers, such as ISPs, that transmit, route, or provide connections for, material through a system or network controlled or operated by or for such service providers (which activities are carried out by service providers defined in section 512(k)(1)(A)) qualify for conditional immunity against copyright liability conferred under section 512(a) provided they meet the following conditions. That is, the transmission carrying any infringing content was initiated by a third party, the carrying of content is an automatic technical process, the recipients of the content are not selected by the service provider, the transient storage of content does not allow access to anyone other than the anticipated recipients and is not maintained for a period longer than what is reasonably necessary for the transmission, routing or provision of connections and the service provider does not modify the content in the course of providing the service.[12] Where these conditions are met, no monetary relief may be awarded against such a service provider, whereas any injunctive relief is limited to those specified in section 512(j)(1)(B)–i.e. to restrain an ISP from providing services to infringing users and to compel the blocking of infringing online locations outside the US.[13]

Section 512(b) applies to 'system caching'. Most internet intermediaries perform caching, which is needed to increase the efficiency of internet transmissions.[14] Thus, when content is made available by a third party, to be transmitted via a service provider's system or network and the storage of third party content for caching is done automatically through a technical process,[15] then such a service provider that is required to cache content is eligible to the safe harbour on the fulfilment of several conditions.[16] These conditions include the implementation of a notice and takedown mechanism whereby copyright owners may inform a service provider of the availability of cached infringing content, upon which the service provider must expeditiously remove, or disable access to, the cached infringing content, provided that the notice also includes a confirmation that either the content has been removed at its source or a competent court has ordered the removal of such content at its source.[17] This type of notice and takedown is not controversial as the notice received by the service provider only needs to be acted upon when the infringing content has been removed at its source by the relevant hosting

service or a court has independently determined that the content is infringing. This means that by the time an intermediary is called upon to act on a notice received under this limb of the DMCA safe harbour, the original content has been removed at its source leaving caching unnecessary or a court has determined the illegality of the content–both cases justifying the removal of cached content.[18]

Sections 512(c) and (d) are applicable to content hosting and information location services respectively. Hosts[19] and information location tools (or search engines)[20] store and link third party online content. These intermediaries perform a crucial, yet more controversial, role in connecting content with internet users. Unlike the provision of internet access (that merely connects users to the network) and caching (that is an internal technical process often invisible to internet users), hosting and information location services play a more significant and direct role in making online content available to internet users. Without hosts, content simply cannot exist. Without search engines, content simply cannot be found. In that sense, copyright owners (and perhaps anyone aggrieved by the transmission of illegal online content) might argue that hosts and search engines should play a greater role in keeping the internet free from illegal content, including those that infringe intellectual property rights. This attitude is clearly visible in the way the DMCA safe harbour is structured.

Thus, a content host that has no 'actual knowledge'[21] of the infringing nature of content stored on its platform, or is unaware of any 'facts or circumstances'[22] from which such illegality is apparent (also known as 'red flag' knowledge),[23] and takes steps to expeditiously remove such infringing content[24]–in particular through a notice and takedown[25] process that it has in place–becomes eligible for the safe harbour, provided that no direct financial benefit is derived from the infringing activity in circumstances where the content host has control over such infringing activity.[26] In the case of a search engine the rules applicable to content hosts apply with only one change–that is, it would be sufficient for the search engine to simply remove the link to the infringing material or website that facilitates such infringing activity.[27]

However, what is to be noted is that unlike in the case of removing cached content, the notice and takedown mechanism applicable to hosts and search engines requires the removal of infringing content solely based upon the information made available in a notice of claimed infringement[28] provided by a copyright owner (unless, of course, there are other circumstances where a service provider's actual knowledge or awareness of the infringing material or activity can be inferred). This requires the intermediary to make a determination as to the validity of the copyright owner's claim that content which is either hosted or linked by that intermediary is infringing–a determination that must be made to facilitate the *expeditious* removal, or de-linking, of infringing material, a condition that needs to be fulfilled in order to benefit from the safe harbour.[29]

It is this aspect of the notice and takedown process that is most controversial–as a private entity (an intermediary) must determine whether content, either hosted or linked by it, infringes copyright based solely on a claim made by a copyright owner (the very individual that seeks the removal, or de-linking, of content), whereas, such a determination affects the rights and interests of the individual who generated or shared the content sought to be taken down. While this *extra-judicial* process is useful in order to keep pace with the speed and spread of the internet, it questions the procedural fairness, transparency, and accountability of the notice and takedown process that ultimately determines the rights and interests of parties to a dispute

arising from the creation, storage and sharing of online content. Thus, although it is contended that the DMCA safe harbour aims at ensuring the growth of internet technology, which will only be constrained if liability is directed at internet intermediaries, the notice and takedown aspect of the safe harbour may in fact constrain the free flow of information–the very purpose for which the internet was developed.

The Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression in his report to the United Nations Human Rights Commission had succinctly identified the potential conflict of notice and takedown practices with the exercise of free speech on the internet:

> …while a notice-and-takedown system is one way to prevent intermediaries from actively engaging in or encouraging unlawful behaviour on their services, it is subject to abuse by both State and private actors. Users who are notified by the service provider that their content has been flagged as unlawful often have little recourse or few resources to challenge the takedown (La Rue, para 42).

Indeed, the notice and takedown process that DMCA 512 envisions has also attracted criticism in the academic world, the most common argument being that the notice and takedown process chills free speech.[30]

However, the DMCA has built in certain mechanisms or safeguards to achieve a more accountable and transparent notice and takedown process. These safeguards include the counter notification mechanism and the safeguards against misrepresentations.

The safeguards

The DMCA safe harbour provides an important safeguard to intermediaries that implement notice and takedown mechanisms. That is, they are assured general immunity from any liability that might arise from the good faith removal, or de-linking, of infringing material "regardless of whether the material or activity is ultimately determined to be infringing"[31] by a court of law. This is protection that is akin to the safeguard made available under the Communications Decency Act,[32] which arguably is aimed at encouraging intermediaries to innovate in the sphere of detecting and monitoring infringing content and activity. However, the immunity for good faith takedowns is qualified. That is, where a service provider removes alleged infringing content, pursuant to a notice of claimed infringement as provided for under section 512(c)(1)(C) (which is directed at hosts), the general immunity will not be afforded unless the service provider does the following:

(a) takes reasonable steps to notify the subscriber that it has removed the material,

(b) upon receipt of a counter notification from the person responsible for the material that was removed, promptly provides the person who served the notice of claimed infringement with a copy of the counter notification, and informs that person that it will replace the removed material, and

(c) replaces the removed material in not less than 10, and no more than 14, business days following receipt of the counter notice, unless the person who submitted the notice of claimed infringement informs that an action has been filed seeking a court order to restrain the person responsible for the alleged infringing material from

> engaging in infringing activity relating to the material on the service provider's system or network.[33]

The process set out above could be described as a counter notice and restoration mechanism, which allows aggrieved parties whose content was removed to challenge a notice of claimed infringement. This is an important mechanism that has the potential of preventing abuse on the part of copyright owners. A point to note is that unless a service provider complies with the counter notice and restoration mechanism, the immunity that is otherwise conferred on the service provider will not apply. Thus, in a situation where perfectly legitimate content is mistakenly taken down by a service provider pursuant to a notice of claimed infringement, the failure on its part to restore the said content upon receiving a counter notification will open the service provider to liability in a suit at the instance of the aggrieved party. Notably, however, the requirement to notify the subscriber about the removal of content and comply with the counter notification procedure only apply in circumstances where a service provider removes content consequent to a notice of claimed infringement (conferring it actual knowledge of a potential infringement). This safeguard does not therefore apply to circumstances where a service provider removes content on its own motion upon acquiring actual or red-flag knowledge of an infringement other than through a notice of claimed infringement.

The second safeguard the DMCA provides is against those who misrepresent particulars in notices of claimed infringement or counter notifications. Thus, section 512(f) provides that any person who *knowingly materially misrepresents* that any material or activity is infringing, or that material or activity was removed or disabled by mistake or misidentification, shall be liable for damages incurred by the alleged infringer, any copyright owner or service provider that is injured by the misrepresentation. In *Online Policy Group v Diebold* (2004), the US District Court (Northern District of California) citing the Black's Law Dictionary defined the phrase 'knowingly materially misrepresents'. Accordingly, 'knowingly' means that the sender of the notice knew or should have known of the misrepresentation, or would have had no substantial doubt about the misrepresentation if it had acted in good faith, whereas a misrepresentation is material, if it affects the service provider's response to the notice (*Online Policy Group v Diebold*, 2004, p.1204). In *Lenz v Universal Music* (2015), the US Court of Appeals (9th Cir.) considered the scope of section 512(f) in deciding that a copyright owner ought to have had a *subjective good faith belief* that the alleged infringing content or activity does not constitute fair use before serving a notice of claimed infringement.[34] While section 512(f) itself does not refer to 'good faith', it appears that section 512(c)(3)(A)(v), dealing with the contents of notices of claimed infringement, requires copyright owners to make a statement under penalty of perjury that the notice is served with the good faith belief that use of the material (complained of) is not authorised by the copyright owner. A similar requirement is imposed in respect of counter notifications, where the notifying party must possess a good faith belief that the service provider had taken down content owing to a mistake or misidentification of the material that was removed.[35] Thus, where a copyright owner or a subscriber lacks the requisite good faith belief, and yet goes on to serve a notice of claimed infringement or counter notification (as the case may be) on a service provider triggering the removal or restoration of content, this would amount to a material misrepresentation. The trial court's judgement, which was affirmed by the Court of Appeals, in *Lenz v Universal Music* (2015) explains the interface between good faith and the provision on misrepresentations:

> An allegation that a copyright owner acted in bad faith by issuing a takedown notice without proper consideration of the fair use doctrine thus is sufficient to state a misrepresentation claim pursuant to Section 512(f) of the DMCA (*Lenz v Universal Music*, 2008, pp1154-55).

Although the safeguard enshrined in section 512(f) is no doubt useful, it appears that establishing that a party 'knowingly' made a 'material' misrepresentation is a fairly heightened burden. This is because it is generally difficult to prove a negative—that a party lacked good faith.[36] To make things more equal, it may be appropriate to shift the burden onto those who assert good faith to prove it.[37] Moreover, good faith is not displaced and a "copyright owner cannot be liable simply because an unknowing mistake is made, even if the copyright owner acted unreasonably in making the mistake" (*Michael Rossi v MPAA*, 2004, p.1005). Despite these issues, however, the structured approach, and stringent requirements, of DMCA 512 regarding notices of claimed infringements and counter notifications, have proven to be useful in preventing abuse in contrast to the model adopted in the EU under the E-Commerce Directive, which does not set out such formal requirements in its safe harbour provisions.[38]

Approach to online copyright enforcement in Singapore

The US-Singapore Free Trade Agreement and the amendment to Singapore's copyright law

Copyright law in Singapore is governed by the Copyright Act 1987 (CA 1987). The CA 1987 was amended in 2004 by the introduction of the Copyright (Amendment) Bill 2004[39] to give effect to Singapore's obligations under the US–Singapore Free Trade Agreement (US-Singapore FTA) which was signed between the two governments on 6 May 2003. Chapter 16 of the US-Singapore FTA included provisions on the protection of intellectual property, and more specifically dealt with enforcement matters.[40] Para 22 of Art 16:9 provides for the limitation of liability for service providers carrying out the four categories of functions set out in DMCA 512–i.e. (1) transmitting, routing or providing connections for material without modification of its content, or the intermediate and transient storage of such material in the course thereof, (2) caching carried out through an automatic process, (3) storage at the direction of a user of material residing on a system or network controlled or operated by or for the service provider and (4) referring or linking users to an online location by using information location tools, including hyperlinks and directories.[41] The conditions upon which immunity is granted[42] and the definition of 'service providers'[43] are identical to those found in DMCA 512.

The speech of the Minister of Law, Professor S Jayakumar, when the Copyright (Amendment) Bill 2004 was read for the second time in Parliament, made it patently clear that the amendment to the CA 1987 was specifically meant to address Singapore's obligations under the US-Singapore FTA, which included the introduction of a safe harbour for intermediaries that operate on the internet:

> The amendments in the Bill address the needs of both copyright owners and users in this new environment. These changes in the Bill will also further strengthen Singapore's position as an attractive location for copyright-based activities. Several of the amendments in the Bill also relate to our obligations under the United States-Singapore Free Trade Agreement (Singapore Parliamentary Report, 2004, column 1042).

The outcome of the amendment was the introduction of an entirely new part (i.e. Part IXA) to the CA 1987 titled 'Works, or other subject-matter, in electronic form' to specifically deal with 'network service providers' and to provide for a safe harbour that limits their liability.

The Singapore copyright safe harbour

To a significant degree, the Singapore copyright safe harbour is identical to DMCA 512, shielding network service providers from copyright liability upon fulfilling certain specific conditions set out therein, although there are some notable deviations that are considered below.

Definition of 'network service providers'

Although DMCA 512, as well as the US-Singapore FTA, use the term 'service provider' in defining the types of intermediaries to which the safe harbour applies, the Singaporean safe harbour instead uses the phrase 'network service provider' in defining its scope. Although on its face, the addition of the prefix 'network' seems to narrow down the scope of the safe harbour, the wording and structure adopted in defining the phrase is identical to what is found in the DMCA. Thus, a network service provider for the purposes of sections 193B, 193DDA and 193DDB of the CA 1987 means "a person who provides services relating to, or provides connections for, the transmission or routing of data."[44] This category explicitly refers to intermediaries that provide internet access services–i.e. ISPs. For the purposes of the other provisions of Part IXA of the CA 1987, a network service provider means "a person who provides, or operates facilities for, online services or network access" and also includes a network service provider that fits the description of ISPs.[45]

Yet, the recent decision of the Singapore High Court in *RecordTV v MediaCorp* (2009) casts some doubt about the breadth of this definition. In this case, RecordTV provided a service via its website that allowed users to select TV programmes (based on weekly schedules) telecasted by MediaCorp so that when the telecast actually takes place it is automatically recorded on RecordTV's servers for viewing by the user that requested the service. The question to be decided, in an action by RecordTV alleging groundless threats of copyright infringement by MediaCorp,[46] was whether RecordTV infringed MediaCorp's copyright in copying the copyrighted content for storage in its servers. The High Court concluded that RecordTV did infringe copyright, which then gave rise to the further question as to whether RecordTV was exempted from liability under the copyright safe harbour. There are two points that must be made in this regard. First, referring to the definition of 'network service provider' in section 193A of the CA 1987, Andrew Ang J observed:

> In arguing that it is a "network service provider", as the term is commonly understood, the plaintiff does some violence to the English language. In common parlance, a network service provider is a business or organisation that sells bandwidth or network access by providing direct access to the Internet. In other words, a network service provider *provides* the *service* of enabling a person to connect to a *network* (*RecordTV v MediaCorp*, 2009, para 90).

Notably, Andrew Ang J's construction of the phrase 'network service provider' refers only to intermediaries that 'sell bandwidth or network access' enabling a person to 'connect' to the internet–i.e. ISPs. However, this observation was made in the context of RecordTV's defence under section 193B, which exempts the activity of 'Transmission, routing and provision of

connections'. Accordingly, it would be reasonable to assume that the observation made by the judge was specifically in relation to the first category of network service providers, and not the second broader category. Additionally, when considered in light of the motivations behind introducing Part IXA of the CA 1987 (to align Singapore's copyright law with the requirements of the US-Singapore FTA) and Professor Jayakumar's parliamentary speech during the second reading of the Copyright (Amendment) Bill 2004, it becomes clear that 'network service provider' ought to be given a much broader definition to include at least 'hosts':

> …the provisions on Network Service Provider liability in this Bill are intended to make NSPs more pro-active in assisting copyright owners to protect and enforce their rights. In the current Act, NSPs enjoy blanket immunity for acts of infringement of copyright or copyright infringing material on their networks. In other words, NSPs are completely absolved of responsibility for such acts or infringing material that they host or provide access to. The provisions in this Bill serve to create a better balance between the interests of rights owners and NSPs, by ensuring that the benefit of immunity that NSPs can enjoy are now accompanied by certain responsibilities (Singapore Parliamentary Report, 2004, column 1050).

Secondly, and perhaps more problematically, Andrew Ang J made the following remark– "the safe harbour provisions exist to protect *bona fide* network service providers from inadvertently being found liable for copying copyrighted material" (*RecordTV v MediaCorp*, 2009, para 91). Unfortunately, the High Court did not provide much guidance on what it meant by 'bona fide', except to suggest that RecordTV made copies of copyrighted programming and therefore it was not considered one that is bona fide (Seng, 2010, p.41). Even though an appeal was lodged against the High Court's decision,[47] the Court of Appeal did not consider the High Court's treatment of the safe harbour provisions in light of its finding that RecordTV did not commit an infringement in doing what it did. As such, the qualification made by the High Court, that the safe harbour applies to 'bona fide' network service providers did not receive any clarification from the land's highest court. Commenting on the High Court's interpretation of 193A, Seng (2010, p.41) has observed:

> The court did not explain what it meant by a "bona fide" network service provider, only that as RecordTV made copies of the rightholders' programming, it was not considered one that is bona fide. With respect, however, this judicial gloss placed on the safe harbor defenses appears to be erroneous and is not supported by the plain language of section 193A.

One approach to overcoming the uncertainty is to tie the High Court's conclusion–that RecordTV's business model resulted in itself making copies of copyrighted content (albeit at the request of its customers)–with the 'bona fide' requirement. Thus, where an intermediary adopts a business model that is purposefully directed at committing or facilitating copyright infringements, it is unlikely to be regarded as a 'bona fide' network service provider. Construing the 'bona fide' requirement in this way will not conflict with the operation of the copyright safe harbour. After all, such intermediaries arguably receive a direct financial benefit from the infringements in circumstances where they have a right and ability to control the infringing activity.[48] Affording such an interpretation would not deprive *neutral* and *passive* intermediaries from claiming eligibility to the copyright safe harbour.

If, however, 'bona fide' is defined too narrowly, possibly resulting in a greater number of intermediaries being deprived of the safe harbour, this will have implications on the practice of notice and takedown. Even though the removal of content at the first instance, upon acquiring actual knowledge of infringing content (e.g. consequent to a notice of claimed infringement), is voluntary (although must be done in order to benefit from the safe harbour),[49] complying with any consequential conditions (including conditions relating to counter notifications and restoration requirements) become mandatory if a network service provider wishes to claim immunity against any liability under any rule of law in respect of any action taken in good faith in relation to the removal or de-linking of content.[50]

Yet, irrespective of whether the safe harbour applies, when an intermediary that hosts, or links, third party content, acquires knowledge about infringing content through a notice of claimed infringement (or otherwise) it is likely that it will remove or de-link the alleged infringing content (as the case may be). This is in view of the incentive to avoid potential liability under substantive copyright law.[51] However, the same incentive of avoiding liability may not exist in relation to compliance with counter notification requirements. This is in view of contractual mechanisms that are often in place between intermediaries and those whose content is removed, or de-linked, that excludes any liability arising from such removal, or de-linking, of content.[52] However, there might be instances where intermediaries remove, or de-link, content generated or shared by parties with whom they have no contractual relations–this is often the case with search engines. Nevertheless, even in the absence of a contractual mechanism to limit liability, such intermediaries might still be motivated to restore, or re-link, content upon receiving a counter notification, in view of the *perceived* risk of liability for failing to do so.[53] There could also be other motivations for intermediaries to comply with counter notifications–e.g. to maintain good relations with their subscribers or customers whose content was removed, or de-linked. Regardless of the motivations and incentives, however, the restoration, or re-linking, of content subject to a good faith counter notice is crucial in maintaining the right balance between the interests of copyright owners and parties that generate and share content on the internet. Yet, unless intermediaries are safeguarded from any ensuing liability towards copyright owners for responding to counter notifications, they may simply ignore counter notifications–which arguably could result in free speech rights and the fair use of copyrighted material being completely disregarded on the internet.

The Singapore copyright safe harbour provides an important safeguard to network service providers that restore, or re-link, content pursuant to a counter notification in the following terms:

> Notwithstanding anything to the contrary in any law (written or otherwise), a network service provider shall not be subject to any liability under any rule of law in respect of any action taken in good faith in relation to—(a) the restoration of an electronic copy of any material to his primary network; or (b) the restoration of access to an electronic copy of any material on any network, if such restoration was done in reliance of any counter notice referred to in subsection (2)(b).[54]

Notably, however, the above safeguard can only be relied upon by network service providers to which the copyright safe harbour applies. Thus, in the event that the 'bona fide' requirement introduced by Andrew Ang J in *RecordTV v MediaCorp* (2009) is applied too narrowly, thus depriving the benefit of the safe harbour to network service providers that are otherwise neutral

and passive, such intermediaries will be placed between a rock and a hard place. The failure to respond to a counter notification could expose the intermediary to liability as against the subscriber whose content was removed or de-linked, whereas responding to a counter notification could give rise to liability as against the copyright owner whose rights were allegedly infringed. Such an outcome must be avoided, as it will not be conducive to the operation of intermediaries on the internet. In the circumstances, a Singaporean court, if not Parliament, must set the record straight by either clarifying that the High Court in *RecordTV v MediaCorp* (2009) was wrong to introduce a 'bond fide' requirement (when such language is absent in the statute itself) or providing a clear definition of what 'bona fide' means in determining the character of network service providers to which the safe harbour should apply.

Knowledge requirement to trigger takedowns

CA 1987 refers to several levels of knowledge upon which a network service provider is required to remove, or de-link, alleged infringing content in order to benefit from the safe harbour. As with the US's DMCA, the Singaporean safe harbour, compels hosts and information location tools (but not ISPs) to remove, or de-link, infringing material upon gaining the requisite knowledge of an infringement–failing to do so resulting in the safe harbour becoming inapplicable.

Network service providers that engage in system caching must remove alleged infringing content from the cache upon receiving a notice of claimed infringement,[55] containing information identical to what is required under the US's DMCA.[56] As such, the removal of cached infringing content is only triggered on the basis of a service provider's actual knowledge of an infringement, which is imputed only upon a notice being served.

To maintain eligibility to the safe harbour, a network service provider that provides hosting or information location (or search) services must remove, or delink, infringing content in three specific scenarios. First, when it acquires *actual knowledge* that content hosted or linked by it infringes copyright.[57] Secondly, when a network service provider acquires *knowledge of facts or circumstances* which would lead inevitably to the conclusion that material hosted or linked by it infringes copyright.[58] This envisages removal of infringing content on the basis of constructive, or red flag, knowledge. Thirdly, when a network service provider is served with a notice of claimed infringement by a copyright owner (or someone authorised).

Although three levels of knowledge–i.e. actual, red flag and notice-based knowledge–regarding infringing material may be imputed, notice-based knowledge is simply a means of imputing actual knowledge. However, when the CA 1987 was amended in 2004 to incorporate the copyright safe harbour, a network service provider was required to expeditiously remove or disable access to alleged infringing content *only* if it was furnished "in the prescribed manner with a notice [of claimed infringement] in the prescribed form."[59] Yet DMCA 512, which was the basis for the Singapore copyright safe harbour, requires notices to be only 'substantially' in the prescribed form for it to be an 'effective notice'.[60] Thus, the notice requirements imposed under the Singapore copyright safe harbour was stricter than its US counterpart. However, the position changed in 2005 when the CA 1987 was further amended.[61] Accordingly, at present, when a network service provider is "furnished in the prescribed manner with a notice in, *or substantially in accordance with*, the prescribed form," it must act to remove or disable access to alleged infringing content.[62] Thus, it is clear that where a network service provider is furnished with a notice of claimed infringement that is substantially in the prescribed form that

would be sufficient to impute actual, if not red flag, knowledge of an infringement on the part of the service provider.[63]

There is, however, a further point that needs to be addressed. That is whether a notice of claimed infringement that is neither fully, nor substantially, in the prescribed form is sufficient to impute knowledge of an infringement on the part of a network service provider. It would appear that the response, at least in Singapore, would be in the negative in view of section 193D(3) of the CA 1987, which reads:

> For the purposes of subsection (2), a notice purportedly made by the owner of the copyright in the material or under the owner's authority which is not a notice referred to in subsection (2)(b)(iii)[64] […] shall not be considered in determining whether the network service provider has acquired any knowledge referred to in subsection (2)(b)(i) or (ii).[65]

Essentially, a notice of claimed infringement that does not fully, or substantially, comply with the prescribed requirements cannot impute either actual or red flag knowledge of an infringement on the part of a network service provider.

Interestingly, the position under DMCA 512 is somewhat different. Thus, where a notice does not substantially comply with *all* the requirements of section 512(c)(3)(A), yet nevertheless does comply substantially with the requirements set out in section 512(c)(3)(A)(ii)-(iii),[66] unless the service provider promptly attempts to contact the person making the notification or takes other reasonable steps to assist the notifying party to substantially comply with *all* the requirements of section 512(c)(3)(A), that service provider may be imputed with knowledge of infringements for the purposes of determining whether the safe harbour applies.[67] This means that the receipt of a notice that does not substantially comply with *all* of the statutory requirements may still be enough to impute knowledge on the part of a service provider in limited circumstances.[68] In *Capitol Records v MP3Tunes* (2013), the US District Court (Southern District of New York) held that something less than a formal takedown notice may establish red flag knowledge.[69]

Whereas, in Singapore, unless a copyright owner complies substantially with *all* the prescribed requirements of a notice of claimed infringement, a network service provider cannot be imputed with knowledge of infringements pursuant to such an incomplete notice. Thus, in Singapore, the burden imposed on copyright owners regarding compliance with the prescribed conditions is stricter than what is found under the US's DMCA.

Counter notices and restoration

There are some striking differences between the Singapore copyright safe harbour and DMCA 512 in the way counter notifications operate. Under the DMCA, to maintain the general immunity conferred on a service provider against any liability that may ensue as a result of the removal of content,[70] the service provider must comply with three specific conditions, the aim of which are to facilitate counter notifications and the restoration of content.[71] Notably, however, these conditions apply *only* to service providers that *host* third party content in respect of the removal of content pursuant to a notice of claimed infringement.[72]

In contrast, under the Singapore safe harbour, the conditions to maintain general immunity apply not only in respect of content removed as a result of a notice of claimed infringement,

but also where such removal takes place as a result of the network service provider acquiring actual or red flag knowledge of an infringement.[73] Thus, unlike under the US's DMCA, a network service provider could lose its general immunity if it (1) fails to notify its subscriber of the removal of content and (2) fails to restore content pursuant to a counter notification, even in circumstances where the content was originally removed without a notice of claimed infringement being served on the network service provider.

Moreover, unlike under the DMCA, the conditions that compel counter notification and restoration of content apply in respect of information location service providers.[74] Thus, where access to infringing content is disabled upon an information location service provider acquiring actual or red flag knowledge, or pursuant to a notice of claimed infringement, counter notification and restoration procedures must be followed in order for the service provider to benefit from the general immunity conferred under the safe harbour.

Accordingly, the counter notification and restoration process under the Singapore safe harbour is far broader than its US counterpart. This confers greater protection towards subscribers that generate and share content, especially as against overcautious, if not overzealous, network service providers that seek to remove, or disable access to, content upon acquiring the slightest doubt about its legality, even in the absence of a notice of claimed infringement.

Online enforcement of copyright in India

India has adopted a hybrid approach to deal with the liability of internet intermediaries for copyright infringements–two statutes becoming potentially applicable–i.e. the Information Technology Act 2000 (ITA 2000) and the Copyright Act 1957 (CA 1957). Both these statutes have been amended on numerous occasions, some of which dealing directly with the liability of internet intermediaries.[75]

The framework under the ITA 2000

Steering India to meet the challenges of electronic commerce that the twenty-first century was bound to pose, it enacted the ITA 2000 to provide for the "legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, […] to facilitate electronic filing of documents with the Government agencies […] and for matters connected therewith or incidental thereto."[76] The ITA 2000, however, in its original formulation adopted a rather narrow approach in respect of the liability of intermediaries. Section 79, before it was amended in 2009, introduced a safe harbour to shield intermediaries from liability–its heading "[n]etwork service providers not liable in certain cases" hinting this fact. The said provision read as follows:

> …it is hereby declared that no person providing any service as a *network service provider* shall be liable *under this Act, rules or regulations made thereunder* for any third party information or data made available by him *if he proves that the offence or contravention was committed without his knowledge* or *that he had exercised all due diligence to prevent the commission of such offence or contravention* (emphasis added).

The explanation attached to the aforesaid provision clarified that 'third party information' meant "information dealt with by a network service provider *in his capacity as an intermediary*,"[77] while a 'network service provider' was simply equated to an 'intermediary',[78] which was defined in the following terms–"*with respect to any particular electronic message*

means any person who *on behalf of another person receives, stores or transmits* that message or provides any service with respect to that *message*."[79] It appears that when the ITA 2000 was enacted almost two decades ago, it reflected the state of the internet in India in that period of time. Although internet related technologies were more advanced in the West, the developments in India were comparatively slower. In the year 2000, internet services were supplied by a few centralised entities and did not entail the high speed interactive connectivity we see today. In the circumstances, when the term 'intermediary' was originally defined in the ITA 2000, the emphasis was on entities that provided 'connectivity' and 'transmission'. This is quite clear in view of how the definition of 'intermediary' begins (see italicised part of the definition above) with reference to an 'electronic message'. Interestingly, the term 'electronic message' was not defined in the ITA 2000. However, an 'electronic message' reflects something that is being *transmitted* informing the narrow perception of what constituted an intermediary under the original definition. In addition, the term 'stores' that appears in the definition of an 'intermediary' alongside 'receives' and 'transmits' could not have meant the permanent storage of information–but when taken in context must have implied the transient or incidental storage in the course of receiving or transmitting information. Based on this analysis, the original definition of 'intermediary' seems to have been limited to internet intermediaries that provided the core service of connecting and transmitting–namely, ISPs.

Moreover, section 79 (in its original formulation) expressly sought to limit a network service provider's liability "under *this Act, rules or regulations made thereunder*". The ITA 2000 itself, before it was amended, did not impose any liability on intermediaries. Whereas, based on how the original safe harbour was worded, it did not seek to limit the liability of an intermediary arising under any other statute or the common law–and this includes liability for copyright infringements. In any case, since the definition of 'intermediary' was very narrow, it was unlikely that liability of any kind could have been imposed on the class of intermediaries envisaged under the ITA 2000 in its original formulation. This in effect would have made the safe harbour both redundant and superfluous in practice.

However, in 2009, the ITA 2000 was amended.[80] Accordingly, an 'intermediary' is now defined as:

> *with respect to any particular electronic record*, 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*.[81]

Whereas, section 2(1)(t) of the ITA 2000 defines 'electronic record' to mean "data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche." Under the new approach, it would appear that the ITA 2000 refers to a broad range of intermediaries, no doubt including ISPs, hosts and information location tools (or search engines)–the essential criteria being that they must deal with third-party content (i.e. content not generated or created by them). This definition of 'intermediary' to a great extent is comparable with the corresponding definition in the US's DMCA safe harbour.

The IT (Amendment) Act 2009 also brought about significant changes to section 79 of the IT Act 2000. Section 79(1) now provides:

> Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.

It is quite clear that the amended section 79 is broader in several respects in comparison to its previous formulation.

First, the terminology of 'network service provider' has been removed and is replaced by the term 'intermediary'. This change is significant in view of the corresponding amendment that was made to section 2(1)(w) with regard to the definition of 'intermediary'. Moreover, doing away with the narrow language of 'network service provider' confirms the broader application of the section 79(1) safe harbour.

Secondly, the amended provision excludes an intermediary's liability for any *third party information, data*[82] *or communication links*. The last of these terms is not defined in the ITA 2000 itself. However, the Information Technology (Intermediaries Guidelines) Rules 2011 (Intermediaries Guidelines), enacted to supplement the ITA 2000, defines 'communication links' as follows:

> a connection between a hyperlink or graphical element (button, drawing, image) and one or more such items in the same or different electronic document wherein upon clicking on a hyperlinked item, the user is automatically transferred to the other end of the hyperlink which could be another document website or graphical element.[83]

Arguably, the inclusion of the term 'communication links' captures a broader category of content for which the safe harbour extends, evincing the breadth of the new provision.

Thirdly, and perhaps more importantly, section 79(1) applies to two types of activities that intermediaries may engage in–namely, making third party information, data or communication links *available* to internet users, as well as the *hosting* of such third party content. Thus, it is clear that the safe harbour applies not only to intermediaries that engage in providing access to third party content (e.g. ISPs and search engines), but also to hosts that enable the permanent storage of content. This is comparable to the DMCA safe harbour in terms of application and scope.

However, the limitation of liability afforded to intermediaries is subject to several conditions. Section 79(2) sets out three conditions, of which the first two (laid down in paras (a) and (b) to section 79(2)) apply *disjunctively*–i.e. it would suffice for either of the two conditions to be satisfied for an intermediary to benefit from the safe harbour, although the last condition (in para (c)) must be with the conditions in para (a) or (b), whichever applicable.[84] The first of these conditions mandate that the function of an intermediary must be limited to "providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted."[85] This condition arguably applies to ISPs as they provide *access* to communication systems on which information provided by third parties is transmitted or stored.

In terms of the second condition, the intermediary must not have initiated, selected the recipient of, or modified information contained in any transmission.[86] This condition replicates the same requirement that must be satisfied before the safe harbour under the US's DMCA[87] could be applied to ISPs. Therefore, it may be posited that the first two conditions set out in section

79(2), without doubt, apply to ISPs. However, because section 79(2) makes the conditions set out therein applicable to an 'intermediary', it does not differentiate between ISPs, search engines and hosts. As such, although the conditions in the US's DMCA that correspond to those set out in section 79(2)(a) and (b) of the ITA 2000 specifically apply to ISPs, in the Indian context these conditions arguably become relevant even in respect of search engines and hosts. In this regard, the judgement of the Divisional Bench of the High Court of Delhi (divisional bench) in *MySpace v SCIL* (2016), in which section 79 of the ITA 2000 was closely examined, warrants attention.

MySpace operating at *www.myspace.com* was a US based service provider that inter alia permitted subscribing users to upload and store content. The content hosted in this way became accessible to anyone that visited the MySpace website. This aspect of MySpace's service entails the *hosting* of third party content. Super Cassettes Industries Ltd (SCIL) was one of India's largest music companies and owned copyright in over 100,000 songs. The dispute began when SCIL served a legal notice on MySpace on 20 February 2008, requesting the latter to take down (or remove) content that infringed the former's copyright–the legal notice contained a sample list of webpages that displayed the infringing content. Although MySpace responded on 12 March 2008, assuring that the identified infringing content had been taken down and a copyright filter was in place to prevent further infringements, it appears that MySpace was still making available content that infringed SCIL's copyright–which resulted in the legal action. A single judge of the Delhi High Court found that MySpace was *not* entitled to the safe harbour in the ITA 2000 in respect of the alleged copyright infringements.[88] MySpace appealed to a divisional bench of the Delhi High Court.

The first point that the divisional bench had to decide was whether MySpace qualified as an 'intermediary' for the purposes of the ITA 2000. In this regard, the Delhi High Court held that "MySpace […] falls within Section 2(1)(w) and qualifies as an intermediary/Internet service provider because it acts as a "conduit"/portal for information where users can upload and view content" (*MySpace v SCIL*, 2016, para 43). The more controversial point was the second point that had to be decided–i.e. whether MySpace could claim protection from liability under section 79(1) of the ITA 2000. In assessing this point, the divisional bench considered the conditions set out in section 79 that must be fulfilled before an intermediary could claim the benefit of the safe harbour. In respect of the condition set out in section 79(2)(a), the divisional bench concluded that MySpace's function was limited to *providing access* to a communication system over which information made available by third parties is *hosted* (*MySpace v SCIL*, 2016, para 55). Of course, in the case of MySpace, it provided access to its own communication system in which third party-content was hosted. In that sense, it appears that the condition in section 79(2)(a) could be applied not only to ISPs but also to hosts and search engines–as all these intermediaries provide access to a communication system containing content transmitted or hosted by third parties.

As regards the condition set out in section 79(2)(b), the divisional bench observed as follows:

> …under Section 79(2)(b) an intermediary should not initiate the transmission, select the receiver of the transmission and select or modify the information. It is reasonably clear that MySpace complies with the first and second subclauses; it has a "free for all" platform, which by itself does not initiate the sharing feature. While it has created the "share" option that per se does not mean that it "initiates" an action. Content, which is

> shared can be both lawful and unlawful and in any case at a prima facie stage, this Court does not discern that MySpace initiates the transmission; the usage of that feature rests purely in the hands of third party users. Similarly, it does not choose its audience/ receiver. Anyone with Internet access can open its website and be a receiver/viewer of the data being transmitted. Now, on the third sub-clause of whether MySpace selects or modifies information, this court at a prima facie stage finds that firstly the modification is to the format and not to the content and secondly even the process of modifying the format is an automatic process without either MySpace's tacit or expressed control or knowledge. In the circumstances, this Court concludes that MySpace prima facie complies with the requirements of Section 79(2)(b) (*MySpace v SCIL*, 2016, para 56).

In essence, the divisional bench applied the conditions set out in section 79(2)(b) to a host and concluded that the conditions were met. This is an important aspect in which the Indian safe harbour deviates from the DMCA 512, as the cumulative conditions set out in section 79(2)(b) are those that normally apply to ISPs in the US context. Whereas in India, as the decision in *MySpace v SCIL* (2016) demonstrates, the conditions set out in section 79(2)(b) of the ITA 2000 have also been applied to a host, with the possible application to search engines as well.

The upshot of all this is that for an intermediary, *whether it is an ISP, search engine or host,* to qualify for the Indian safe harbour, must satisfy either of the first two conditions set out in section 79(2) of the ITA 2000–i.e. that the function of the intermediary concerned is limited to providing access to a communication system *or* that it did not initiate, select the recipient of, or modify information contained in a transmission–'transmission' being interpreted broadly by the divisional bench of the Delhi High Court in *MySpace v SCIL* (2016) to include information hosted and stored temporarily. Generally speaking, however, ISPs, hosts and search engines are likely to satisfy both these conditions.

Section 79(2)(c) sets out the third condition that an intermediary must comply with to qualify for the safe harbour—a condition that is not to be seen in the DMCA safe harbour. That is, for the safe harbour to apply to an intermediary it must observe 'due diligence' while discharging its duties. In this regard, the divisional bench in *MySpace v SCIL* (2016, para 57) suggested that the Intermediaries Guidelines had to be considered. Rule 3(1) of the Intermediaries Guidelines provides that an "intermediary shall publish the rules and regulations, privacy policy and user agreement for access or usage of the intermediary's computer resource by any person." In addition, Rule 3(2) requires such rules and regulations or user agreements to inform users of an intermediary's services that they shall not "host, display, upload, modify, publish, transmit, update or share any information that" comes within the confines of paras (a) to (i) of Rule 3(2). Importantly, this includes information that "infringes any patent, trademark, copyright or other proprietary rights."[89] Rule 3(3) provides that an intermediary shall not *knowingly* host any information that is prohibited under Rule 3(2) paras (a)-(i). Interestingly, the Delhi High Court, in *Christian Louboutin v Nakul Bajaj* (2018), observed that compliance with the due diligence guidelines set out in the Intermediaries Guidelines does not conclusively determine whether a service provider should be treated as an intermediary to which the safe harbour applies. In this regard, the Court observed:

> Following the guidelines may in certain cases satisfy that the online market place is behaving as an intermediary but the same is not conclusive. What is lawful or unlawful depends on the specific statute being invoked and the Guidelines cannot be considered

> as being exhaustive in their manner of application to all statutes (*Christian Louboutin v Nakul Bajaj*, 2018, para 71).

Arguably, the Delhi High Court seems to be hinting that the applicability of the safe harbour may require intermediaries not only to remain neutral and passive service providers but also to take on more responsibility in suppressing unlawful content, such as the incorporation of filters or similar technologies—a trend that has recently received legal recognition in the EU.[90]

While section 79(2) of the ITA 2000 set out conditions that an intermediary must satisfy to become eligible for the safe harbour, section 79(3) sets out instances where the safe harbour will not apply. Arguably, section 79(3) is aimed at ensuring that the safe harbour applies only in respect of truly neutral and passive intermediaries. Accordingly, section 79(3)(a) provides that an intermediary that conspires, aids, abets or induces an unlawful act on the part of another, shall not be eligible for the safe harbour. Interpreting section 79(3)(a) of the ITA 2000, the Delhi High Court in *Christian Louboutin v Nakul Bajaj* (2018, para 68) observed:

> Section 79(3)(a) limits the exemption only to those intermediaries i.e. platforms and online market places who do not aid or abet or induce the unlawful act. *Any active contribution by the platform or online market place completely removes the ring of protection or exemption which exists for intermediaries under Section 79*.

In essence, the effect of the aforesaid provision is that a service provider whose conduct actively contributes towards the commission of an unlawful act, including intellectual property infringements, on the part of its users will not be regarded as an intermediary for the purposes of the safe harbour—thus ensuring the applicability of the safe harbour to truly natural and passive intermediaries.[91]

On the other hand, section 79(3)(b) provides that the safe harbour will not apply if:

> upon receiving *actual knowledge* […] that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit [an] *unlawful act*, the intermediary *fails to expeditiously remove or disable access to that material on that resource*… (emphasis added).

Rule 3(4) of the Intermediaries Guidelines supplements the aforesaid provision by providing that an intermediary on whose computer system information is stored, hosted or published, upon obtaining actual knowledge *by itself* or through a *notification in writing* (including an email with electronic signature) by the affected person about any information prohibited under Rule 3(2) paras (a)-(i) shall "act within thirty six hours and where applicable, work with user or owner of such information, to disable such information." A clarification issued in 2013 by the Government of India suggests that what an intermediary must do within 36 hours of receiving a notice is to acknowledge receipt of the complaint/grievance and initiate appropriate action.[92] As such, although an intermediary must expeditiously remove or disable access to unlawful information upon being notified, this need not be done within 36 hours of receiving a notice, although Rule 3(11) provides that complaints must be redressed within one month from the date of receipt.[93]

From the language of both section 79(3)(b) of the ITA 2000 and Rule 3(4) of the Intermediaries Guidelines, it is clear that they provide the basis for a notice and takedown regime in India.

However, there are some important observations that must be made when comparing section 79(3)(b) to the DMCA safe harbour.

First, the Indian safe harbour applies horizontally in respect of *all* unlawful material, which includes material that violate intellectual property rights. In light of this feature, the Indian safe harbour is closer to the EU's safe harbour, which may have been what prompted the divisional bench in *MySpace v SCIL* (2015, para 41) to observe that "the Indian "safe harbour" provisions for online intermediaries are similar to the [E-Commerce Directive], not the DMCA."

Secondly, unlike the DMCA 512 (and even the EU's safe harbour), it is unclear whether the conditions set out in section 79(3)(b) is limited in its application to typical hosts that engage in the permanent storage of third party content. There are some references in section 79(3)(b) that lead to the impression that the provision is directed at permanent storage and not transient or incidental storage (or caching). For example, the words 'residing', 'controlled by the intermediary' and 'remove or disable access' appearing in section 79(3)(b) have been borrowed directly from section 512(c)(1) of the DMCA applicable to *hosts*. Moreover, Rule 3(4) of the Intermediary Guidelines expressly refer to information "stored or *hosted*" which seems to imply that the rule applies to intermediaries that host third party content. In addition, a perusal of section 79 as a whole suggests that where the legislature intended to refer to temporary forms of storage (as in the case of transient and incidental storage or caching), then the phrase 'temporarily stored' has been used.[94] As such, it might be argued that the condition that requires the removal or disabling of third party content upon the acquisition of actual knowledge of its illegal nature applies to hosts that engage in a more permanent form of content storage.

Thirdly, the language of section 79(3)(b) is somewhat vague about its applicability to search engines or information location service providers. While the DMCA 512 treats information location tools separately (in section 512(d)), this is not the case with the Indian safe harbour. However, it may be posited that section 79(3)(b) does apply to search engines, because it uses the phrase 'communication link', which has been defined to include 'hyperlinks'[95] that search engines use in linking internet users to third party websites. As such, for a search engine (or information location service providers) to become entitled to the section 79(1) safe harbour, it must disable access to the unlawful content upon acquiring actual knowledge of its existence.

Fourthly, in order to become entitled to the Indian safe harbour, intermediaries are obligated to remove or disable access to unlawful material only upon acquiring *actual knowledge* of its existence. Consequent to the Intermediaries Guidelines, actual knowledge may be imputed on an intermediary upon its own conduct ("by itself") or through a notice served on it by the affected party.[96] While this corresponds with the DMCA 512 to some degree–the obligation to remove alleged unlawful content under the Indian safe harbour does not arise where an intermediary acquires constructive (or red-flag) knowledge.[97] This approach diffuses some of the uncertainties surrounding red-flag knowledge, which make it difficult for intermediaries to assess when they have acquired the requisite awareness of facts or circumstances from which the unlawful nature of content should be apparent. In fact, the use of a red-flag standard under the US's DMCA has been subject to some criticism for want of certainty.[98] For this reason, the Indian notice and takedown regime, which is premised on a standard of *actual knowledge* should lead to more certain outcomes, albeit this is to some extent diluted, as neither section 79, nor the Intermediaries Guidelines, provide much guidance about the contents and form of an

effective notice[99]–the only requirement being that it must be served in writing or by email accompanied by an electronic signature.[100]

Lastly, it is noteworthy that the safe harbour regime under the ITA 2000 does not envisage the possibility of counter notices. This is problematic in the copyright context, as there is no opportunity for third parties to assert fair use (or fair dealing in the Indian context) or free speech rights. This is yet another feature of the Indian safe harbour that distances it from the US's DMCA and places it closer to the EU's safe harbour, which does not recognise the possibility for counter notices.

The fifth condition that an intermediary must satisfy before it becomes eligible for the safe harbour has been set out in section 79(3)(a) of the ITA 2000. Accordingly,

The safe harbour under the CA 1957

The CA 1957 provides for the protection and enforcement of copyright in India. By an amendment in 2012,[101] significant changes were made to the CA 1957, which included the incorporation of two new provisions to deal with the liability of intermediaries. These new provisions were introduced as part of the general provision in the CA 1957 providing for exceptions to copyright–i.e. section 52.

The relevant parts of section 52 are reproduced below:

> (1) The following acts shall not constitute an infringement of copyright, namely:--"
>
> (a) […]
>
> (b) the transient or incidental storage of a work or performance purely in the technical process of electronic transmission or communication to the public;
>
> (c) transient or incidental storage of a work or performance for the purpose of providing electronic links, access or integration, where such links, access or integration has not been expressly prohibited by the right holder, unless the person responsible is aware or has reasonable grounds for believing that such storage is of an infringing copy:
>
> Provided that if the person responsible for the storage of the copy has received a written complaint from the owner of copyright in the work, complaining that such transient or incidental storage is an infringement, such person responsible for the storage shall refrain from facilitating such access for a period of twenty-one days or till he receives an order from the competent court refraining from facilitating access and in case no such order is received before the expiry of such period of twenty-one days, he may continue to provide the facility of such access.

Both paras (b) and (c) of section 52(1) refer to *transient* or *incidental* storage of a work or performance. Referring to the Black's Law Dictionary (7th edn), the divisional bench in *MySpace v SCIL* (2016, para 59) observed that "[t]ransient means any work which is *temporary or impermanent* and incidental would mean something *subordinate to something of greater* importance" (emphasis added). It is clear that section 52(1)(b) and (c) refer to *caching* activities

of intermediaries–a specific category within the DMCA safe harbour.[102] On that basis, the divisional bench in *MySpace v SCIL* (2016, para 59) excluded the applicability of section 52(1)(b) or (c) to hosting activities that MySpace carries out:

> Hosting and storing data, as observed earlier does not qualify to be referred to as incidental or transient data. The nature of the data being uploaded is of a permanent type, one which is accessible whenever demanded or searched for. These are the major functions and any storage which is of a temporary form aiding in the better performance of the main function would be covered under Section 52(1)(b) and (c). Under the current circumstances of the appeal, the content in question is the permanent kind.

The divisional bench also drew a distinction between section 52(1)(b) and (c) in the following way:

> Reference is made to Section 52(1)(b), which provides absolute immunity to intermediaries, who are the backbone of the Internet, i.e. whose functions are core to the working of the Internet like telecommunication carriers and Internet service providers (ISPs). On the other hand Section 52(1)(c) provides a limited immunity to the intermediary. This immunity is available to intermediaries such as search engines, social media websites etc. *so long as they have no reasonable belief that the content hosted infringes copyright* (*MySpace v SCIL*, 2016, para 22) (emphasis added).

Thus, according to Court, section 52(1)(b) applies to intermediaries that are the *backbone* of the internet such as ISPs, whereas section 52(1)(c) applies to search engines and social media sites–although it is unclear how this conclusion was reached. In this regard, it is instructive to consider the corresponding provision in Singapore's copyright statute. Section 38A of the CA 1987[103] provides that "the copyright in a work is not infringed by the making of a temporary or transient reproduction of the work if–(a) the reproduction is made incidentally as part of the technical process of making or receiving a communication; and (b) the act of making the communication itself does not constitute an infringement." The parliamentary debates in respect of the Bill that introduced this exception to Singapore's copyright law suggest that this provision is concerned with temporary copies of a work made at the *user's end*. There is no reference to ISPs when this provision was considered in the parliamentary debates. The relevant part of the parliamentary debate is reproduced below:

> First, amendments to the provisions dealing with temporary reproductions and user caching. […] when a user receives or makes an electronic communication, or surfs the Internet, incidental copies of material are automatically *made on the user's computer*. *For example, when an Internet user visits a website, a copy of the website content is automatically made by the user's computer, primarily to speed up the loading of the webpage on a repeat visit.* These copies are made automatically, and involve no direct action by the user. *As such, the user should not be held liable for any copyright infringement occurring under such circumstances.* Therefore, the existing Copyright Act exempts the making of such incidental copies from copyright infringement. Clauses 2, 4, 9 and 15 of the Bill amend sections 38A, 107E, 193E and 252D respectively to clarify, for avoidance of doubt, that the exemption only applies to short-lived incidental copies, and not to long-lasting copies even if they are made automatically (Singapore Parliamentary Report, 2005, columns 800-801) (emphasis added).

What may be gleaned from the parliamentary debates (extracted above) is that section 38A of Singapore's CA 1987 is concerned *exclusively* with temporary reproductions of works that take place when *internet users* lawfully gain access to such works via their internet browsers or other means. However, section 52(1)(b) of the Indian copyright statute contains an important difference. That is, it applies to the temporary reproduction of works purely in the technical process of electronic transmission *or communication to the public*. While 'electronic transmissions' corresponds to 'making or receiving a communication' that appears in the Singaporean provision, the Indian provision, in addition, refers to 'communication to the public'. This significantly changes the dynamic of the Indian provision–after all, the communication of works to the public is an exclusive right vested on copyright owners, and there is no reason to exempt internet users who interfere with that right. On the other hand, when intermediaries perform their technical functions, they may incidentally communicate works to the public. Arguably, the purpose of section 52(1)(b) is to exempt intermediaries from incurring copyright liability for any temporary storage of works when they engage in the technical process of transmitting or communicating to the public–although it also arguably covers internet users insofar as their browsing activities result in the temporary reproduction of works. Thus, even though the divisional bench in *MySpace v SCIL* (2016) did not provide any reasons for holding that section 52(1)(b) applied to intermediaries such as ISPs, the analysis above supports that finding.

In contrast, section 52(1)(c) applies to the context of temporary reproductions of works made in the course of an intermediary's function of providing *electronic links, access or integration*. According to the divisional bench in *MySpace v SCIL* (2016), this provision applies to a broader range of intermediaries ("search engines, social media websites etc.") whose conduct results in the transient or incidental storage of material in the course of providing electronic links, access or integration. However, the distinction between the scope of sections 52(1)(b) and (c) is not very clear. Although the divisional bench in *MySpace v SCIL* (2016) limited the application of section 52(1)(b) to intermediaries that comprise the *backbone* of the internet (ISPs being cited as an example), the language adopted in section 52(1)(c) might arguably extend to ISPs as well, since the latter provision applies to intermediaries that engage in the conduct of providing *access*–ISPs clearly come within the scope of access providers. Unfortunately, the Standing Committee Report on the Copyright (Amendment) Bill 2010[104] (the Bill that introduced sections 52(1)(b) and (c)) does not add much clarity on the matter. The lack of clarity is problematic, because section 52(1)(b) provides complete immunity to ISPs in respect of their technical functions, whereas section 52(1)(c) provides conditional immunity that is premised on the adoption of a notice and takedown process. Thus, insofar as ISPs are concerned, if their conduct becomes caught up by both sections 52(1)(b) and (c), there could be uncertainty about their liability for the temporary reproduction of works that occurs in the course of their technical functions.

In fact, the judgement of a single judge bench of the Bombay High Court in *Eros International v BSNL* (2016) adds to the uncertainty. This case concerned the Bollywood super hit film, 'Dishoom', unauthorised copies of which were made available on a number of websites before the film's official release in India. Eros International, which owned the copyright in the film, sought an order from the Bombay High Court compelling 42 ISPs operating in India to block access to 134 URLs[105] pointing to websites that contained unauthorised copies of the film. In the course of the judgement, Patel J made the following observation:

> In other words, upon the Plaintiffs drawing the attention of any of the Defendants Nos. 1 to 42 to any specific verified URL […] which is shown to be a link to a page containing links for illicit downloads, display or streaming of the film in question, these Defendants will first restrict access to that URL or web link (not to an entire website) as required by Section 52(1)(c) and for the 21 day period mentioned in that section. For any continuance of the page-specific URL-block, the Plaintiffs must apply to Court, and liberty is expressly reserved to them to do so (*Eros International v BSNL*, 2016, para 24).

In essence, the Bombay High Court referred to section 52(1)(c) of the CA 1957 as providing a basis for compelling ISPs to *block* access to online locations (or websites) containing infringing material. Nothing in section 52(1)(c) expressly provides a basis for website blocking orders.[106] However, section 52(1)(c) does require an intermediary to *refrain from facilitating access* to infringing material that becomes temporarily stored in the course of providing electronic links, access or integration, once an intermediary receives a written complaint from a copyright owner. While this requires an intermediary to implement a notice and takedown process in respect of infringing material that is temporarily stored in an intermediary's network or platform, arguably, a written complaint in respect of specific infringing material would have the effect of the intermediary being expressly prohibited from providing electronic links, access or integration in respect of the identified infringing material. In effect, this would require the intermediary that is served with a notice to ensure that it no longer processes the infringing content even if the outcome of such processing is the temporary storage of the infringing material. Failure to do so would disentitle that intermediary from the safe harbour afforded by section 52(1)(c). In the case of ISPs, one way of ensuring that they do not process infringing material identified in a written complaint is to block access to the infringing source–which would have the effect of preventing internet users from accessing the source of infringement eliminating the need on the ISP's part temporarily store the infringing material in any way for the purpose of processing. Affording such an interpretation to section 52(1)(c) could dismiss any conflict between Patel J's approach in *Eros International v BSNL* (2016) and the subsequent decision of the divisional bench of the Delhi High Court in *MySpace v SCIL* (2016).

Although section 52(1)(b) provides general immunity to intermediaries in respect of the transient or incidental storage of infringing material purely in the course of their technical functions, in cases where such transient or incidental storage takes place for the purpose of providing electronic links, access or integration, the safe harbour is displaced in two situations. The first is where an intermediary is *aware* that the transient or incidental storage is of an infringing copy. This assumes a standard of actual knowledge. Importantly, such actual knowledge may be imputed when an intermediary receives a written complaint. In this situation, the safe harbour will remain applicable provided the intermediary refrains from facilitating access to any infringing material that had been temporarily or incidentally stored in the intermediary's platform or network. Once a written complaint is received, however, to retain eligibility to the safe harbour, the intermediary must ensure that it does not process the material identified in the complaint–as this would be deemed as providing electronic links, access or integration in circumstances *expressly prohibited* by a copyright owner. The second instance where the safe harbour will be displaced is where an intermediary *has reasonable grounds for believing* that the transient or incidental storage is of an infringing copy. This is analogous to red flag knowledge under the US's DMCA.

Although section 52(1)(c) introduces a notice and takedown requirement for intermediaries for the purposes of the safe harbour, its implementation is vastly different to what is found in the DMCA. The first point of deviation concerns the knowledge standard. The section 52(1)(c) safe harbour applies in respect of an intermediary that has no actual or red flag knowledge that content stored is infringing. This seems to incorporate an *objective* knowledge standard premised on 'reasonable grounds for belief'[107] in addition to an actual knowledge standard that is *subjective* and notice based. This approach, however, is markedly different from the DMCA's approach in two ways. First, for an intermediary dealing with cached material to benefit from the DMCA safe harbour, it must expeditiously remove, or disable access to, alleged infringing material upon receiving a notice of claimed infringement.[108] Thus, in the US context, an intermediary would become disentitled to the safe harbour *only* upon acquiring *actual knowledge* of the existence of infringing material stored on a temporary basis through a notice. Secondly, removal of cached material is required only when it is established that the material at its source has already been removed or a court order exists that compels its removal or disablement at the source.[109] Arguably, these are two useful control mechanisms aimed at preventing abusive takedown notices, which are lacking in the Indian approach.

Secondly, there are also differences as to how the notice and takedown process operates. Under the DMCA, once the cached material is removed, there is no requirement or process to restore that material. Arguably, this is because removal of cached content is only mandated where the material at the source has been removed, making the cached content redundant. In contrast, in India, the proviso to section 52(1)(c) of the CA 1957 requires intermediaries to continue to provide access to cached material after 21 days of a complaint/notice, unless the complaining party obtains an order from the competent court. When the proviso is read with Rule 75(2)(f) of the Copyright Rules 2013 (Copyright Rules), it becomes clear that the court order referred to in the proviso must be an order in an action between the copyright owner (or licensee) and the person responsible for uploading the infringing material. This could be described as a safeguard, somewhat akin to the counter notice and restoration mechanism under the DMCA, although its utility is questionable. After all, section 52(1)(c) deals with material stored on a *temporary* basis (i.e. cached), and unlike in the case of material that is permanently hosted, restoring cached content may be technically difficult, if not impossible. In any case, caching does not entail the long-term storage of material. As such, in practical terms, there is no logic to requiring an intermediary to restore access to material stored on a temporary basis in cases where the copyright owner fails to furnish a court order. There is no point in restoring access to material that might not even be in existence at the end of the 21-day window. In fact, the DMCA safe harbour does not impose an obligation on intermediaries to restore cached content that was removed pursuant to a notice of claimed infringement.

Thirdly, unlike under section 79(3) of the ITA 2000, notices/complaints under the proviso to section 52(1)(c) must comply with a standard set out in the Copyright Rules 2013 (Copyright Rules). Accordingly, Rule 75(2) of the Copyright Rules provide that for the written notice/complaint to be effective under section 52(1)(c) of the CA 1957, it must contain the following particulars:

(a) a description of the work with sufficient information to identify the work in which copyright subsists.

(b) details establishing that the complainant is the owner or licensee of copyright in the identified work.

(c) details establishing that the transient or incidental copy of the work is an infringing copy and that none of the exceptions to copyright protection apply.

(d) details of the location where the temporary storage of the work is taking place.

(e) the identity of the person, if known, who is responsible for uploading the material infringing the copyright in the work of the complainant.

(f) undertaking that the complainant shall file an infringement suit in the competent court against the person responsible for uploading the infringing material and produce the orders of the competent court having jurisdiction within a period of 21 days from the date of the notice/complaint.[110]

These requirements are comparable to those under the DMCA 512,[111] although there are some points of deviation. For instance, a notice under the DMCA requires the notifying party to include information sufficient to allow the intermediary to contact the complaining party,[112] a physical or electronic signature of the complaining party[113] and a statement under penalty of perjury that the information contained in a notice is accurate.[114] These requirements, although important, are not to be found in Rule 75(2) of the Indian Copyright Rules.

Harmonious reading of the ITA 2000 and CA 1957

One of the questions that the divisional bench in *MySpace v SCIL* (2016) had to decide was whether the ITA 2000 and CA 1957 had to be read harmoniously. This was because SCIL's claim against MySpace was premised on section 51(a)(ii) of the CA 1957, whereas MySpace relied on the safe harbour in section 79(1) of the ITA 2000 (as amended). Since the provision upon which MySpace's liability was premised and the provision that excluded MySpace's liability were located in two distinct statutes, the divisional bench had to determine whether one prevailed over the other, or on the other hand whether a harmonious interpretation must be afforded.

Section 51(a)(ii) of the CA 1957 provides that:

> Copyright in a work shall be deemed to be infringed when any person, without a licence granted by the owner of the copyright […] permits for profit any place to be used for the communication of the work to the public where such communication constitutes an infringement of the copyright in the work, unless he was not aware and had no reasonable ground for believing that such communication to the public would be an infringement of copyright.

The above provision is aimed at persons who provide premises to be used by third parties engaged in the communication of protected copyright works to the public, although in *MySpace v SCIL* (2016, para 34) it was argued, and the Court accepted, that it applied even to virtual spaces–"MySpace owns a website where third party users upload and view content. In a sense, the appellant is a provider of a place, albeit virtual, to communicate various kinds of works." Of course, for liability to arise, the person who provides the place to be used by third parties

must have *reasonable grounds for believing* that the communication of the works to the public would amount to an infringement. As such, there was no necessity for *actual knowledge* of infringements for liability to arise–it being sufficient to possess *constructive knowledge* from which a *reasonable man* would arrive at such a belief about infringements (*MySpace v SCIL*, 2016, para 35). However, what was necessary is specific awareness of infringements and not mere general awareness (*MySpace v SCIL*, 2016, para 35). Thus, in this regard, the divisional bench held that only a notice that specifically identified the infringing work and its location could impute the requisite knowledge on MySpace to trigger liability–"[i]t is only when MySpace has specific or actual knowledge or when it has reasonable belief, based on information supplied by SCIL and if despite such knowledge or reasonable belief it fails to act can it be held liable for infringement" (*MySpace v SCIL*, 2016, para 38).

Yet, although a sufficiently detailed and specific notice of infringement is adequate to impute the requisite knowledge for the purposes of section 51(a) (ii) of the CA 1957, it is clear that a notice is not a prerequisite to trigger liability under that provision. All that is required is a reasonable belief of infringement, and this could arise even without a specific notice. But at the same time, where a party is an intermediary that hosts third party content, it must be noted that sections 79(1) and (3) will apply. As a result, a host will become disentitled to the safe harbour *only* where it acquires *actual knowledge* of an infringement and *fails* to remove the underlying infringing content. As such, under section 51(a)(ii) of the CA 1957, a *reasonable belief* of infringement is a sufficient condition for a host's liability, whereas under the ITA 2000 *actual knowledge* of an infringement is required to displace the safe harbour. This means there is a mismatch in the knowledge standards between a liability imputing provision in the CA 1957 and the liability limiting provision in the ITA 2000.

It is within this backdrop that the divisional bench in *MySpace v SCIL* (2016) considered the implications section 81 of the ITA 2000, which provides that "[t]he provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force." Importantly, when the ITA 2000 was amended in 2009, a proviso was added to section 81 to the following effect:

> Provided that nothing contained in this Act shall restrict any person from exercising any right conferred under the Copyright Act, 1957 (14 of 1957) or the Patents Act, 1970 (39 of 1970).

In this regard, the divisional bench observed that "[w]hat prompted Parliament to amend Section 79 still remains a speculation *but the deliberate act of adding the proviso to Section 81 could only lead one to assume that the Parliament intended to not disturb the rights of copyright or patent holders in light of the 2008 amended provisions to the IT Act*" (*MySpace v SCIL*, 2016, para 46) (emphasis added). The Court went on to hold that "Sections 79 and 81 of the IT Act and Section 51(a)(ii) of the Copyright Act have to be read harmoniously" (*MySpace v SCIL*, 2016, para 40). A harmonious reading of these provisions was provided by the division bench when it concluded that "Section 51(a)(ii), in the case of internet intermediaries contemplates *actual knowledge* and not general awareness. Additionally, to impose liability on an intermediary, conditions under Section 79 of the IT Act have to be fulfilled" (*MySpace v SCIL*, 2016, para 68) (emphasis added).

While this no doubt leads to a harmonious interpretation of the statutes that come into play when intermediaries become involved in copyright infringements, requiring *actual knowledge*

for the purposes of section 51(a)(ii) in determining the liability of internet intermediaries is a classic example of internet exceptionalism[115]–online actors being treated more favourably than their offline equivalents, mere *constructive knowledge* being enough to trigger liability in the case of the latter. In addition, the harmonious reading afforded by the divisional bench also lends itself to an act of judicial law making–after all, this approach simply ignores the constructive knowledge requirement that section 51(a)(ii) *expressly* refers to.

Lastly, achieving harmony between the two statutes may not always be straightforward. Consider the transient or incidental storage of material. Given the breadth of the section 79(1) safe harbour (in the ITA 2000), it may be stated with confidence that it applies to intermediaries in relation to their functions that result in the transient or incidental storage of material. Since the condition set out in section 79(3)–which requires the removal of infringing stored material upon notice–applies in relation to content that is permanently stored or *hosted*, temporary storage or cached content does not give rise to any notice and takedown requirement under the ITA 2000. However, section 52(1)(c) of the CA 1957 requires intermediaries to remove infringing content stored on a temporary basis upon being put on notice. As such, the liability of an intermediary in respect of the transient or incidental storage infringing material would depend on the statute the intermediary elects to utilise in support of its defence. Unfortunately, since the divisional bench in *MySpace v SCIL* (2016) was concerned with MySpace's activities that resulted in the *hosting* of infringing material, the Delhi High Court did not have the opportunity to consider this eventuality. Unless the legislature directly addresses this issue, whether a harmonious interpretation of the two statutes is at all possible in this specific scenario will solely depend on the willingness of Indian judges to innovate.

Comparative summary and conclusion

The table below provides a summary of the key features of the Singaporean and Indian safe harbours and compares them with the approach under the US's DMCA.

	US, DMCA 512	**Singapore, CA 1987**	**India, ITA 2000 and CA 1957**
Definition of intermediaries	A 'service provider' has been defined in two tiers. The first expressly refers to ISPs, while the second refer to any other provider of an online service, which is broad enough to capture search engines and hosts.	Textually comparable to the two pronged definition under the US'DMCA. However, in *RecordTV v MediaCorp* (2009) the Singapore High Court introduced a 'bona fide' requirement that a network service provider must satisfy before it qualified for the safe harbour. On appeal, the Court of Appeal did not consider the provisions of the safe harbour because it overruled the findings of the High Court as regards the copyright liability of the defendant service provider–making it unnecessary to consider the provisions of the safe harbour. As such, there is no guidance about what the High Court meant	The ITA 2000 originally provided a very narrow definition for the term 'intermediary' to mainly include entities that engaged in the transmission of 'electronic messages', while section 79(1) which set out the safe harbour, albeit superficially, narrowed the scope of the term 'intermediary' even further by equating it with 'network service provider'. However, in 2009, the ITA 2000 was amended so that a broad range of service providers, including ISPs, search engines and hosts, were brought within the definition of an 'intermediary'.

		when it introduced the requirement of 'bona fide'.	The CA 1957 does not provide a definition for the term 'intermediary', but through amendments in 2012, two provisions were introduced into the CA 1957 (i.e. section 52(1)(b) and (c)), to deal with the transient and incidental storage of content–which captured system caching activities carried out by certain intermediaries.
Nature of Knowledge (of infringement) required to trigger action	For caching activities, an actual notice identifying the existence of infringing content is required. For hosting and information location service providers, three tiers of knowledge (of infringements) apply. Actual knowledge, red flag knowledge and notice-based knowledge. However, notice-based knowledge is arguably a means of imputing either actual or red flag knowledge. Even where a notice does not fully, or substantially, comply with the requirements set out in the DMCA, a service provider *may* be imputed with knowledge in limited circumstances. Generalised knowledge about an infringement insufficient to impute liability.	For caching activities, identical to the DMCA. For hosting and information location service providers, identical to the DMCA–in that the same three-tier knowledge standard applies. However, a notice that does not fully, or substantially, comply with the requirements set out in the Copyright Regulations 2005 cannot be used to impute either actual or red-flag knowledge. Generalised knowledge about an infringement insufficient to impute liability.	India follows a two-prong approach under the ITA 2000 and the CA 1957. The ITA 2000 safe harbour applies an actual knowledge standard in respect of its notice and takedown process. The statute does not lay down any formal requirements concerning the form of notice required to impute actual knowledge, except that the notice must be in writing. The ITA 2000 does not provide for a constructive, or red flag, knowledge standard. The CA 1957 refers to both actual and red flag knowledge standards, although a written notice is required to trigger the notice and takedown process. The CA 1957 is supplemented by the Copyright Rules 2013, which provide in greater detail about the contents of a notice referred to under the statute (i.e. section 52(1)(c) proviso). The judgement in *MySpace v SCIL* (2016) provides the much needed clarity as to the requirements of actual notice leading up to the actual knowledge of infringing content. Generalised knowledge about an infringement insufficient to impute liability.
Takedown procedures	For caching activities, once a service provider receives a notice, removal of infringing content	For caching activities, takedown procedures are identical to the DMCA.	Takedown procedures set out under the ITA 2000 and the CA 1957 are unique. Unlike in the US or Singapore, the

	becomes obligatory to maintain eligibility to the safe harbour, but only where the content at its source has been removed, or a court has ordered for the material to be removed. For hosting and information location service providers to maintain eligibility to the safe harbour, they become obligated to remove, or disabling access to, infringing material upon acquiring actual or red flag knowledge of an infringement, or receiving a notice of infringement substantially in the prescribed form.	For hosting and information location service providers, takedown procedures are identical to the DMCA, except that a notice that does not at least substantially comply with the prescribed form does not obligate the removal, or de-linking, of any content–such non-compliant notices being insufficient to impute any knowledge on the part of a service provider.	statute does not draw a distinction based on the type of activity carried out by service providers. The ITA 2000 requires an intermediary to act within 36 hours after receiving a notice, although the process of taking down need not be completed within 36 hours. The CA 1957 requires an intermediary to take down infringing content stored on a temporary basis for 21 days after receiving a complaint/notice. The removal of cached content becomes permanent in the event there is no court order following such complaint. Whereas, at the end of the 21-day window, if no court order is presented, the intermediary must restore access to the content that was removed.
Counter notice and restoration procedures	Upon the removal of content consequent to a notice of claimed infringement, service providers that host third party content are required to notify the party whose content was removed and restore the content if a counter notification is received. Failure to do so will deprive service providers of the general immunity afforded by the safe harbour. Notably, the restoration obligation is limited to situations where content was removed consequent to a notice.	The position in Singapore is different. Service providers must comply with counter notification and restoration procedures in all instances where content is removed–whether removal was consequent to a notice or otherwise. In addition, unlike under the DMCA, information location service providers are also bound by this condition.	Neither the ITA 2000, nor the CA 1957, sets out a counter notification and restoration process of the type found under the DMCA or the Singapore copyright safe harbour. However, the CA 1957 provides for a restoration process in respect of material that was stored on a transient or incidental basis but was removed, although the trigger for restoration is the absence of a court order in favour of the copyright owner within 21 days of the complaint/notice (and not a counter notification).

On a comparison, it appears that the Singapore copyright safe harbour is very much aligned with the US's DMCA 512. This is not surprising, as the Singaporean safe harbour was introduced specifically to comply with obligations under the US-Singapore FTA. However, the Singapore safe harbour contains certain distinct features that arguably provide a much better balance between the rights of copyright owners and the interests of content producers and intermediaries. These features are–(1) the stricter knowledge standard: ie non-compliant notices incapable of imputing either actual or red flag knowledge of infringements on intermediaries and (2) the counter notification and restoration requirement that applies not only

to hosts but also to search engines (information location service providers) and applicable in all circumstances in which content is removed or de-linked.

In comparison to both the US and Singapore, the existing framework in India is complex by the presence of two regimes–one under the ITA 2000 and the other set out in the CA 1957. The Indian approach, however, is in many ways unique. One such unique feature pertains to the knowledge requirement. In India, the removal of content is premised on an *actual knowledge* standard primarily derived from a notice of infringement/complaint served on the intermediary at the instance of the aggrieved right holder. This eliminates the uncertainties surrounding red flag knowledge, which is present in both the US and the Singaporean contexts. Another unique aspect of the Indian approach relates to the additional responsibilities imposed on intermediaries. Thus, unlike under the DMCA or the Singapore safe harbours, the Intermediaries Guidelines 2011 brought into force in terms of the ITA 2000 provide for *due diligence* requirements, which mandate certain specific steps that intermediaries must adopt in the interests of right holders.

However, India's hybrid approach lags behind in certain respects. For instance, although the ITA 2000 and the Intermediaries Guidelines 2011 set out a 36-hour timeframe within which an intermediary must act upon receiving a notice from an aggrieved party, a subsequent clarification issued by the Government of India in 2013 states that it would suffice for an intermediary to merely acknowledge receipt of a notice within that timeframe. Whereas, the Intermediaries Guidelines of 2011 suggest that intermediaries could take up to a month to redress a complaint, which arguably would include the removal of any infringing material. Such an approach may not be suitable in light of the pace at which material is transmitted on the internet, which requires the expeditious removal of infringing content. Moreover, the absence of a counter notification and restoration mechanism is a significant drawback. This is problematic in relation to the removal of hosted material, as it does not provide internet users whose content is taken down a formal process to challenge abusive or erroneous takedowns. Whereas, the restoration process envisaged under the CA 1957 is also problematic, as it concerns cached content in respect of which there is no real need for a restoration mechanism.

As a way forward, the existing framework in India requires rethought and reshaping. While the unique and innovative features of the Indian approach should be retained, a more structured and consolidated approach to the liability and immunity of internet-based intermediaries is needed in the interest of substantive and procedural certainty and clarity. In this regard, there is much that Indian legal draftsmen could learn from their counterparts in the 'little red dot'.

NOTES

[1] Title II of the DMCA, i.e. the Online Copyright Infringement Liability Limitation Act, introduced a safe harbour (codified at 17 U.S.C. §512) for internet intermediaries that shielded them from copyright liability provided they met certain conditions set out therein.

[2] See, *Sega v Maphia* (1996).

[3] On the issue of direct infringement the judge observed that "Sega has not shown that Sherman himself uploaded or downloaded the files, or directly caused such uploading or downloading to occur. The most Sega has shown is that Sherman operated his [bulletin board service], that he knew infringing activity was occurring, and that he solicited others to upload games. However, whether Sherman knew his [bulletin board service] users were infringing on Sega's copyright, or encouraged them to do so, has no bearing on whether Sherman directly caused the copying to occur" (*Sega v Maphia*, 1996, p.932).

[4] As regards contributory infringement, the judge observed that "[j]ust because Sherman is not liable for direct infringement, however, does not mean that he is free from liability. Although the Copyright Act does not expressly

impose liability on anyone other than direct infringers, courts have long recognized that in certain circumstances, liability for contributory infringement will be imposed" (*Sega v Maphia*, 1996, p.932).

[5] 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 (E-Commerce Directive). Art.12(1) provides complete immunity to ISPs on similar lines to the DMCA 512. Art.13(1) deals with caching, whereas Art.14(1) provides conditional immunity to hosts. Interestingly, the EU's safe harbour does not deal with information location tools or search engines, which is a significant deviation from its US counterpart.

[6] 17 U.S.C. §512(a).

[7] 17 U.S.C. §512(b).

[8] 17 U.S.C. §512(c).

[9] 17 U.S.C. §512(d).

[10] The US District Court (Central District of California) came to a similar finding in *Hendrickson v Amazon* (2003).

[11] 17 U.S.C. §512(i)(1). Section 512(i)(2) defines standard technical measures as measured utilised by copyright owners to identify or protect copyrighted works.

[12] 17 U.S.C. §512(a)(1)–(5).

[13] The provisions in the DMCA that confer immunity to ISPs are identical to those available in the EU's corresponding safe harbour (Art.12 of the E-Commerce Directive).

[14] See, Senate Report (1998, p.42).

[15] 17 U.S.C. §512(b)(1)(A)-(C).

[16] 17 U.S.C. §512(b)(2)(A)-(E).

[17] 17 U.S.C. §512(b)(2)(E).

[18] The provisions in the DMCA that confer immunity to intermediaries engaging in caching activities are identical to those found in the EU's E-Commerce Directive (Art.13).

[19] Most ISPs provide hosting services as well (e.g. Singtel in Singapore). However, there are companies that engage exclusively in hosting content and these include typical web-hosts (e.g. Host Papa and Go Daddy).

[20] The most popular ones include Google, Yahoo and Bing.

[21] 17 U.S.C. §512(c)(1)(A)(i).

[22] 17 U.S.C. §512(c)(1)(A)(ii).

[23] In *Viacom v YouTube* (2012), the US Court of Appeals (2nd Cir.), clarified the relationship between red flag and actual knowledge in the following way:

> "The difference between actual and red flag knowledge is thus not between specific and generalized knowledge, but instead between a subjective and an objective standard. In other words, the actual knowledge provision turns on whether the provider actually or subjectively knew of specific infringement, while the red flag provision turns on whether the provider was subjectively aware of facts that would have made the specific infringement objectively obvious to a reasonable person" (para 43).

This approach was followed in subsequent cases–e.g. the first instance decision of the US District Court (Southern District of New York) in *Capitol Records v Vimeo* (2013). On appeal, although the US Court of Appeals (2nd Cir.) did recognise and apply the standard for red flag knowledge as set out in *Viacom v YouTube* (2012), the Court explained that the "reasonable person" referred to in the standard must be an "ordinary person—not endowed with specialized knowledge or expertise concerning music or the laws of copyright" (*Capitol Records v Vimeo*, 2016, p.94). Arguably, this approach has heightened the burden of establishing red flag knowledge on the part of service providers.

[24] 17 U.S.C. §512(c)(1)(A)(iii).

[25] 17 U.S.C. §512(c)(1)(C).

[26] 17 U.S.C. §512(c)(1)(B).

[27] 17 U.S.C. §512(d). See also, Senate Report (1998, p.48), which provides an explanation as to how the notice and takedown mechanism operates in respect of search engines.

[28] The elements of which are provided for in section 512(c)(3).

[29] As with the DMCA, the EU safe harbour provides for the immunity of hosts from liability (Art.14), according to which immunity is conditional upon the expeditious removal of unlawful content upon a host acquiring actual knowledge or awareness of an illegality. However, unlike the DMCA, the EU safe harbour does not expressly deal with information location tools (such as search engines).

[30] See e.g. Seltzer (2010), Wilson (2010), Mostert & Schwimmer (2011) and Adler (2011).

[31] 17 U.S.C. §512(g)(1).

[32] 47 U.S.C. §230(c)(2):

> "No provider or user of an interactive computer service shall be held liable on account of–(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or (B) any action taken to enable or make available to

information content providers or others the technical means to restrict access to material described in paragraph (1)."

[33] 17 U.S.C. §512(g)(2)(A)-(C).

[34] In this regard, the judge observed as follows:

"The DMCA already requires copyright owners to make an initial review of the potentially infringing material prior to sending a takedown notice; indeed, it would be impossible to meet any of the requirements of Section 512(c) without doing so. A consideration of the applicability of the fair use doctrine simply is part of that initial review" (*Lenz v Universal Music*, 2015, pp.1133-35).

[35] 17 U.S.C. §512(g)(3)(C).

[36] See, *Karen Dudnikov v MGA Entertainment* (2005, p.1013):

"Because MGA has asserted that it had a good faith belief that the Plaintiffs' auction was an infringement, Plaintiffs have the burden of demonstrating material facts showing otherwise. I agree with Magistrate Judge Coan that Plaintiffs failed to satisfy this burden."

[37] Wilson (2010, pp.631-36) makes this argument in his critique of the good faith standards under the DMCA.

[38] Some empirical evidence exists to suggest that DMCA 512 is less amenable to abuse than the safe harbor incorporated into the E-Commerce Directive–see e.g. Ahlert et. al. (2004) and Nas (2004).

[39] The Bill was later enacted as the Copyright (Amendment) Act 2004 (Act No 52/2004).

[40] US-Singapore FTA, Art 16:9.

[41] US-Singapore FTA, Art 16:9, para 22(b)(i)(A) to (D).

[42] US-Singapore FTA, Art 16:9, para 22(b)(iv), (v) and (vi).

[43] US-Singapore FTA, Art 16:9, para 22(b)(xii).

[44] CA 1987, section 193A(1)–'network service provider', para (a).

[45] CA 1987, section 193A(1)–'network service provider', para (b).

[46] MediaCorp had issued cease and desist letters to RecordTV on two occasions before the latter commenced the action for groundless threats of copyright infringement–see, *RecordTV v MediaCorp* (2009, para 3).

[47] See, *RecordTV v MediaCorp* (2010).

[48] This requirement exists in the DMCA (17 U.S.C. §512(c)(1)(B) and 512(d)(2)), as well as under the Singapore copyright safe harbour (CA 1987, 193D(2)(a)).

[49] CA 1987, section 193D(1)(a) and (b) read with sections 193D(2) and 193D(4) (these provisions lay down takedown requirements in respect of intermediaries that host or link content). Section 193C of CA 1987 deals with system caching and corresponding takedown requirements.

[50] CA 1987, section 193DA(1) read with section 193DA(2).

[51] See e.g. Seltzer (2010, p.186):

"The DMCA does not force service providers to avail themselves of its [safe harbour], but shapes their risk assessment so that almost all do, even in cases where, objectively, no [safe harbour] appears necessary."

[52] It is common for internet-based intermediaries to include wide exemption clauses in their contracts with subscribers. A wide enough exemption clause may allow an intermediary to defend itself against a claim by a subscriber whose content was removed (or de-linked) pursuant to a takedown notice–see, Herman (2013, p.51).

[53] The basis upon which a party, having no contractual relationship with an intermediary, might file an action against that intermediary for the wrongful removal, or de-linking, of content it hosted or linked is unclear. In the absence of a specific cause of action provided under the copyright safe harbour itself, such a claim is likely to be farfetched.

[54] CA 1987, section 193DA(4). This provision is derived from section 512(g)(4) of the DMCA.

[55] CA 1987, section 193D(2)(b).

[56] CA 1987 does not set out the requirements for a valid notice of claimed infringement. These requirements are set out in the Copyright (Network Service Providers) Regulation G.N. No. S 220/2005 (Copyright Regulations 2005). The requirements of a notice of claimed infringement in respect of cached content are set out in Reg.3(2).

[57] CA 1987, section 193D(2)(b)(i).

[58] CA 1987, section 193D(2)(b)(ii).

[59] CA 1987, section 193D(2)(b)(iii). The requirements that a notice of claimed infringement must meet in respect of hosting and information location service providers is set out in Reg.3(2) of the Copyright Regulations 2005.

[60] 17 U.S.C. §512(c)(3)(A). See also, Senate Report (1998, p.46)–"The standard against which a notification is to be judged is one of substantial compliance."

[61] See, Copyright (Amendment) Act 2005 (Act No 22/2005).

[62] The 2005 amendment made a similar change in respect of counter notices as well, so that for a counter notice to be effective it must be in, or substantially in accordance with, the prescribed form (CA 1987, section 193DA(2)(b)).

[63] Such a conclusion can be drawn on US case law interpreting corresponding provisions of the DMCA 512. See e.g. *Perfect 10 v CCBILL* (2007) (knowledge of infringement cannot be imputed on a service provider where it is not served with an 'effective notice') and *ALS Scan v RemarQ Communities* (2001) (a notice that was substantially

compliant with the prescribed requirements is sufficient to impute knowledge of infringements on the part of a service provider).

[64] Section 193D(2)(b)(iii) provides for expeditious removal of content by a network service provider upon receipt of a notice of claimed infringement that is fully or substantially compliant with the prescribed form.

[65] Section 193D(3) applies to network service providers that host third party content. Whereas, section 193D(5), which is identical to section 193D(3), applies to network service providers that engage in linking content (e.g. search engines).

[66] These requirements enable a service provider that is served with a notice to identify the copyrighted work claimed to have been infringed, to identify the infringing content and its location and contact the party serving the notice (complaining party).

[67] 17 U.S.C. §512(c)(3)(B)(i) read with (ii).

[68] For example, where a notice of claimed infringement does not contain a statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorised to act on behalf of the owner of an exclusive right that is allegedly infringed, in circumstances where the notice does comply substantially with requirements in section 512(c)(3)(A)(ii), (iii) and (iv), the service provider's failure to contact the complainant and request substantial compliance with all the statutory requirements pertaining to notices may result in the service provider being imputed with knowledge of infringements in determining its status under the safe harbour.

[69] Interestingly, the position under the EU safe harbour seems to be the same. Thus, in *L'Oréal v eBay* (2011, para 122), the Court of Justice of the European Union (CJEU) explained when an intermediary might be regarded as having acquired awareness of an illegality in the following terms:

> "The situations thus covered include, in particular, that in which the operator of an online marketplace uncovers, as the result of an investigation undertaken on its own initiative, an illegal activity or illegal information, as well as a situation in which the operator is notified of the existence of such an activity or such information. In the second case, although such a notification admittedly cannot automatically preclude the exemption from liability provided for in Article 14 of Directive 2000/31, given that notifications of allegedly illegal activities or information may turn out to be insufficiently precise or inadequately substantiated, the fact remains that such notification represents, as a general rule, a factor of which the national court must take account when determining, in the light of the information so transmitted to the operator, whether the latter was actually aware of facts or circumstances on the basis of which a diligent economic operator should have identified the illegality."

[70] 17 U.S.C. §512(g)(1).

[71] See, above n33, and corresponding text.

[72] 17 U.S.C. §512(g)(2).

[73] CA 1987, section 193DA(1)(i) and (ii).

[74] CA 1987, section 193DA(2)(b)(i) and(ii) .

[75] For sake of convenience, where a statutory provision has been amended, the suffix 'before amendment' will be used when referring to the original provision.

[76] ITA 2000, preamble.

[77] ITA 2000, section 79 explanation (b) (before amendment).

[78] ITA 2000, section 79 explanation (a) (before amendment).

[79] ITA 2000, section 2(1)(w) (before amendment) (emphasis added).

[80] See, Information Technology (Amendment) Act 2009 (IT (Amendment) Act 2009).

[81] ITA 2000, section 2(1)(w) (emphasis added).

[82] The term 'data' is defined as "a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer" (ITA 2000, section 2(1)(o)).

[83] Intermediaries Guidelines, Rule 2(b).

[84] A single judge bench of the Delhi High Court provided such an interpretation because the legislature had introduced an "or" between paras (a) and (b) of section 79(2)–see, *SCIL v MySpace* (2011, para 64.4).

[85] ITA 2000, section 79(2)(a).

[86] ITA 2000, Section 79(2)(b)(i)-(iii).

[87] 17 U.S.C. §512(a)(1)-(3).

[88] See *SCIL v MySpace* (2011).

[89] Intermediaries Guidelines, Rule 3(2)(d).

[90] On 26 March 2019, the European Parliament adopted a new Directive on Copyright in the Digital Single Market, which was formally endorsed by the Council of the EU on 15 April 2019. Once the text of the directive is published on the Official Journal, EU Member States will have 24 months to transpose the new directive into their domestic

legislation. Art.17 of new directive will hold 'online content-sharing service providers' liable for copyright infringement, unless they 'made, in accordance with high industry standards of professional diligence, best efforts to ensure the unavailability of specific works and other subject matter for which the rightholders have provided the service providers with the relevant and necessary information' and 'acted expeditiously, upon receiving a sufficiently substantiated notice from the rightholders, to disable access to, or to remove from, their websites the notified works or other subject matter, and made best efforts to prevent their future uploads'. Compliance with Art.17, which originates from the controversial Art.13 in the European Commission's proposal for the new directive, is likely to require service providers to incorporate filtering technology.

[91] This approach is consistent with how safe harbours are approached in the EU as well. Thus, for instance, in *Google v Louis Vuitton* (2010), the CJEU observed (at para 114):

> "Accordingly, in order to establish whether the liability of a referencing service provider may be limited under Article 14 of Directive 2000/31, it is necessary to examine whether the role played by that service provider is neutral, in the sense that its conduct is merely technical, automatic and passive, pointing to a lack of knowledge or control of the data which it stores."

This approach was followed by the CJEU in *L'Oréal v eBay* (2011, para 113).

[92] See Clarification on the Information Technology (Intermediary Guidelines) Rules 2011 (18 Mar 2013).

[93] Interestingly, in *Avnish Bajaj v State* (2008), a single judge bench of the Delhi High Court held that the removal of unlawful content within the timeframe of 38 hours from the time of notice was inadequate to avoid liability. This case concerned the criminal liability of the managing director of an online platform that facilitated buying and selling over the internet (similar to eBay's online marketplace). The Court found liability on the part of the online platform (i.e. its managing director) although it merely acted as an intermediary and had removed the impugned listing (of a video involving child pornography) within 38 hours of receiving a notice from a concerned citizen. This case, however, was decided before the ITA 2000 was amended.

[94] See e.g. ITA 2000, section 79(2).

[95] Intermediaries Guidelines, Rule 2(b).

[96] Intermediaries Guidelines, Rule 3(4).

[97] In contrast, under the DMCA, in order to become entitled to the safe harbour, an intermediary must remove infringing content in three specific circumstances–i.e. (1) when it acquires actual knowledge, (2) when it acquires constructive or red-flag knowledge or (3) when it is served with an effective notice of claimed infringement. The Indian safe harbour incorporated the first two, but not the last.

[98] See e.g. Brown (2008, pp.457-58), Peguera (2009, p.481), Chang (2010, pp.219-20) and Fisher (2015, p.643).

[99] This could be contrasted with the DMCA which sets out specific requirements for an effective notice (see, 17 U.S.C. §512(c)(3).

[100] See Intermediaries Guidelines, Rule 3(4).

[101] See Copyright (Amendment) Act 2012.

[102] See 17 U.S.C. §512(b). The language used in the DMCA under 'System Caching' is 'temporary' and 'intermediate' storage. The EU's E-Commerce Directive (Art.14(1)) defines 'Caching' as 'temporary' and 'intermediate' storage.

[103] Section 38A applies in respect of *works* in which copyright subsist. Whereas, the same exception is extended to *audio-visual items* in section 107E.

[104] See, Parliament of India (2010, paras 19.1-19.10).

[105] URL stands for Uniform Resource Locator–e.g. http://www.example.com/index.html.

[106] Website blocking orders have been commonplace not only in India but also in other jurisdictions. Indian courts have adopted varying legal approaches to award blocking orders. In *Eros International v BSNL* (2016), the Bombay High Court thought it had jurisdiction to issue a blocking order under section 52(1)(c) of the CA 1957. In *Star India v Haneeth Ujwal* (2014), the Delhi High Court decided that it had inherent powers (at para 17) to compel two government departments to secure compliance of a court order requiring the blocking of a number of websites infringing copyright "by calling upon the various internet service providers […] to block access to the various websites identified by the plaintiffs in the instant suit, or such other websites that may subsequently be notified by the plaintiffs to be infringing its exclusive rights, within three days from the date of receipt of the copy of the order" (at para 21(d)). In *Kamalesh Wasvani v Union of India* (2014), pursuant to a writ petition being filed by an Indian lawyer concerning the widespread availability of online child sexual abuse material, the Supreme Court of India issued an order requiring the Government to take appropriate steps to block access to pornographic websites containing such material. Accordingly, the Indian Government issued an Order on Measures to Curb Child Sexual Abuse Material (No 1(3)/2016-CLFE, 18 April 2017) in terms of which ISPs became obligated to block access to pornographic websites that were already blacklisted by the UK's Internet Watch Foundation. The Indian Government cited section 79(2)(c) of the ITA 2000 read Since then, however, the Government's order had been revoked due to controversy, and the matter is presently pending before the Supreme Court to determine what course of action should be followed. In the EU, website blocking orders have been issued, the basis for which is supplied by two EU directives–Art.8(3) of Directive 2001/29/EC (the Info-Soc Directive, applicable specifically

to the copyright context) and Art.11(third sentence) of Directive 2004/48/EC (Enforcement Directive, applicable generally to the enforcement of intellectual property rights). Given the controversial nature of website blocking, in view of its impact on access to information and free speech, the CJEU's guidance has been sought on numerous occasions to determine the legitimacy of website blocking. See e.g. *Scarlet Extended v SABAM* (2011) and *UPC Telekabel v Constantin Film* (2014).

[107] In the context of secondary copyright infringement, 'reasonable grounds for believing' imputes a standard of knowledge from which "a reasonable person would arrive at the relevant belief (and not merely suspect the relevant conclusion) and allowing for a period of time to evaluate the relevant facts"–see, Aplin & Davis (2017, p.221).

[108] 17 U.S.C. §512(b)(2)(E).

[109] 17 U.S.C. §512(b)(2)(E)(i) and (ii).

[110] Copyright Rules, Rule 75(2)(a)–(f).

[111] 17 U.S.C. §512(c)(3).

[112] 17 U.S.C. §512(c)(3)(iv).

[113] 17 U.S.C. §512(c)(3)(i).

[114] 17 U.S.C. §512(c)(3)(vi).

[115] See, Goldman (2010, p.165).

REFERENCES

Adler, J. (2011). The public's burden in a digital age: Pressures on intermediaries and the privatization of Internet censorship. *Journal of Law & Policy*, 20, 231-265.

Ahlert, C., Marsden, C. & Yung, C. (2004). How 'Liberty' Disappeared from Cyberspace: The Mystery Shopper Tests Internet Content Self-Regulation. Retrieved from http://pcmlp.soc leg.ox.ac.uk/wp-content/ uploads/2014/12/liberty.pdf (Accessed 19 June 2018).

ALS Scan v RemarQ Communities (2001): *ALS Scan Inc v RemarQ Communities Inc* 239 F.3d 619 (2001)

Aplin, T. & Davis J. (2017). *Intellectual Property Law–Text, Cases and Materials* (3rd ed.). Oxford: Oxford University Press.

Ardia, D.S. (2010). Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity Under Section 230 of the Communications Decency Act. *Loyola of Los Angelis Law Review*, 43, 373-506.

Avnish Bajaj v State (2008): *Avnish Bajaj v State* Indlaw DEL 763

Bartholomew, M & Tehranian, J. (2006) The Secret Life of Legal Doctrine: The Divergent Evolution of Secondary Liability in Trademark and Copyright Law. *Berkley Technology Law Journal*, 21, 1363-1420.

Brown, B. (2008). Fortifying the Safe Harbors: Reevaluating the DMCA in a Web 2.0 World. *Berkeley Technology Law Journal*, 23, 437-467.

Capitol Records v MP3Tunes (2013): *Capitol Records Inc v MP3Tunes LLC* 2013 WL 1987225

Capitol Records v Vimeo (2013): *Capitol Records LLC v Vimeo LLC* 972 F.Supp.2d 500 (2013)

Capitol Records v Vimeo (2016): *Capitol Records LLC v Vimeo LLC* 826 F.3d 78 (2016)

Chang, L. (2010). The Red Flag Test For Apparent Knowledge Under the DMCA §512(c) Safe Harbor. *Cardozo Arts & Entertainment Law Journal*, 28, 195-222.

Christian Louboutin v Nakul Bajaj (2018): *Christian Louboutin SAS v Nakul Bajaj and Others* 2018 Indlaw DEL 3372

Clarification on the Information Technology (Intermediary Guidelines) Rules 2011 (18 Mar 2013)

Communications Decency Act in 1996 (US)

Copyright Act 1957 (India)

Copyright Act 1976 (US)

Copyright Act 1987 (Singapore)

Copyright (Amendment) Bill 2004 (Singapore)

Copyright (Amendment) Act 2004 (Singapore)

Copyright (Network Service Providers) Regulation G.N. No. S 220/2005 (Singapore)

Corbis v Amazon (2004): *Corbis Corporation v Amazon.com Inc* 351 F. Supp. 2d 1090 (2004)

Digital Millennium Copyright Act 1998 (US)

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 [2000] OJ L 178/1 (E-commerce Directive)

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society [2001] OJ L 167/10 (Info-Soc Directive)

Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the Enforcement of Intellectual Property Rights [2004] OJ L 157/16 (Enforcement Directive)

Directive on Copyright in the Digital Single Market as adopted by the European Parliament on 26 March 2019 and endorsed by the Council on 15 April 2019.

Eros International v BSNL (2016): *Eros International Media Limited and others v Bharat Sanchar Nigam Limited and others* MANU/MH/1482/ 2016 (26 Jul 2016)

Fisher, H. (2015). Danger in the DMCA Safe Harbors: The Need to Narrow What Constitutes Red Flag Knowledge. *University of Richmond Law Review*, 49, 643-669.

Goldman, E. (2010). The Third Wave of Internet Exceptionalism. In B. Szoka & A. Marcus (Eds.), *The Next Digital Decade: Essays on the Future of the Internet* (pp.165-168). Washington DC: TechFreedom.

Google v Louis Vuitton (2010): Joined Cases C-236/08, C-237/08 and C-238/08, *Google France Sarl v Louis Vuitton Malletier SA* [2010] ECR I-02417

Hendrickson v Amazon (2003): *Hendrickson v Amazon.Com* 298 F. Supp. 2d 914 (2003)

Herman, B. D. (2013). *The Fight Over Digital Rights: The Politics of Copyright and Technology.* Cambridge: Cambridge University Press.

Holland, H. B. (2010). Section 230 of the CDA: Internet Exceptionalism as a Statutory Construct. In B. Szoka & A. Marcus (Eds.), *The next digital decade: Essays on the future of the Internet* (pp.189-208). Washington DC: TechFreedom.

Information Infrastructure Task Force. (1995) *Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property Rights*. Retrieved from https://eric.ed.gov/?id=ED387135 (Accessed 19 June 2018).

Information Technology Act 2000 (India)

Information Technology (Amendment) Act 2009 (India)

Information Technology (Intermediaries Guidelines) Rules 2011 (India)

Kamalesh Wasvani v Union of India (2014): *Kamalesh Wasvani v Union of India* (2014) 6 SCC 705

Karen Dudnikov v MGA Entertainment (2005): *Karen Dudnikov and another v MGA Entertainment Inc* 410 F.Supp.2d 1010 (2005)

La Rue, F. (2011). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, UN Human Rights Council, Seventeenth Session, A/HRC/17/27.

L'Oréal v eBay (2011): Case C-324/09, *L'Oréal SA v eBay International AG* [2011] ECR I-06011

Lenz v Universal Music (2008): *Stephanie Lenz v Universal Music Publishing Inc and others* 573 F.Supp.2d 1150 (2008)

Lenz v Universal Music (2015): *Stephanie Lenz v Universal Music Publishing Inc and others* 801 F.3d 1126 (2015)

Marobie-FL v NAFED (1997): *Marobie-FL Inc v National Ass'n of Fire Equipment Distributors* 983 F. Supp. 1167 (1997)

Michael Rossi v MPAA (2004): *Michael J Rossi v Motion Picture Association of America* 391 F.3d 1000 (2004)

Mostert, F. W. & Schwimmer, M. B. (2011). Notice and takedown for trademarks. *Trademark Reporter*, 101, 249-281.

MySpace v SCIL (2016): *MySpace Inc v Super Cassettes Industries Limited* 2016 Indlaw DEL 5477, 2017 (69) PTC 1 (23 Dec 2016)

Nas, S. (2004). The Multatuli Project ISP Notice & take down. *SANE* [online] 27 Oct 2004. Retrieved from https://www-old.bof.nl/docs/researchpaper SANE.pdf (Accessed 19 June 2018).

Online Policy Group v Diebold (2004): *Online Policy Group v Diebold Inc* 337 F. Supp. 2d 1195 (2004)

Order on Measures to Curb Child Sexual Abuse Material (No 1(3)/2016-CLFE, 18 April 2017)

Parliament of India. (2010). Standing Committee on Human Resource Development, Two Hundred and Twenty Seventh Rajya Sabha, Report on the Copyright (Amendment) Bill 2010. Retrieved from http://164.100.47.5/newcommittee/reports/EnglishCommittees/Committee%20on%20HRD/227.pdf (Accessed 20 June 2018).

Peguera, M. (2009). The DMCA Safe Harbour and Their European Counterparts: A Comparative Analysis of Some Common Problems. *Columbia Journal of Law & the Arts*, 32, 481-512.

Perfect 10 v CCBILL (2007): *Perfect 10 Inc v CCBILL LLC* 488 F.3d 1102 (2007)

Playboy v Frena (1993): *Playboy Enterprises Inc v Frena* 839 F. Supp. 1552 (1993)

RecordTV v MediaCorp (2009): *RecordTV Pte Ltd v MediaCorp TV Singapore Pte Ltd and Others* [2009] SGHC 287

RecordTV v MediaCorp (2010): *RecordTV Pte Ltd v MediaCorp TV Singapore Pte Ltd and others* [2010] SGCA 43

RTC v Netcome (1995): *Religious Technology Center v Netcom On-line Communication Services Inc* 907 F. Supp. 1361 (1995)

Scarlet Extended v SABAM (2011): Case C-70/10, *Scarlet Extended SA v Sociétébelge des auteurs, compositeursetéditeurs SCRL (SABAM)* [2011] ECR-I 11959

SCIL v MySpace (2011): *Super Cassettes Industries Limited v MySpace Inc* C.S(OS) 2682/2008, Delhi High Court (29 Jul 2011)

Sega v Maphia (1994): *Sega Enterprises Ltd v Maphia* 857 F. Supp. 679 (1994)

Sega v Maphia (1996): *Sega Enterprises Ltd v Maphia* 948 F. Supp. 923 (1996)

Seltzer, W. (2010). Free speech unmoored in copyright's safe harbor: Chilling effects of the DMCA on the First Amendment. *Harvard Journal of Law & Technology*, 24, 171-232.

Senate Report. (1998). 105th Congress, 2nd Session, Senate Report No. 105–190 on the Digital Millennium Copyright Act. Retrieved from http://www.gpo.gov/fdsys/pkg/CRPT-105srpt190/pdf/CRPT-105srpt190.pdf (Accessed 19 June 2018).

Seng, D. (2010). *Comparative Analysis of the National Approaches to the Liability of Internet Intermediaries*. Geneva: World Intellectual Property Organization. Retrieved from http://www.wipo.int/publications/zh/details.jsp?id=4144&plang=EN (Accessed 19 June 2018).

Singapore Parliamentary Report. (2004). Parliament No. 10, Session No. 1, Volume No. 78, Sitting No. 7 (16 November 2004). Retrieved from https://sprs.parl.gov.sg/search/topic (Accessed 19 June 2018).

Singapore Parliamentary Report. (2005). Parliament No. 10, Session No. 2, Volume No. 80, Sitting No. 6 (18 July 2005). Retrieved from https://sprs.parl.gov.sg/search/topic (Accessed 20 June 2018).

Star India v Haneeth Ujwal (2014): *Star India Pvt Ltd v Haneeth Ujwal* 2014(60) PTC 504 (Del)

UPC Telekabel v Constantin Film (2014): Case C-314/12, *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH* [2014] Bus LR 541

US–Singapore Free Trade Agreement 2004

Viacom v YouTube (2012): *Viacom International Inc v YouTube Inc* 676 F.3d 19 (2012)

Wilson, B. (2010). Notice, Takedown, and the Good-Faith Standard: How To Protect Internet Users From Bad-Faith Removal of Web Content. *St Louis University Public Law Review*, 29, 613-637.