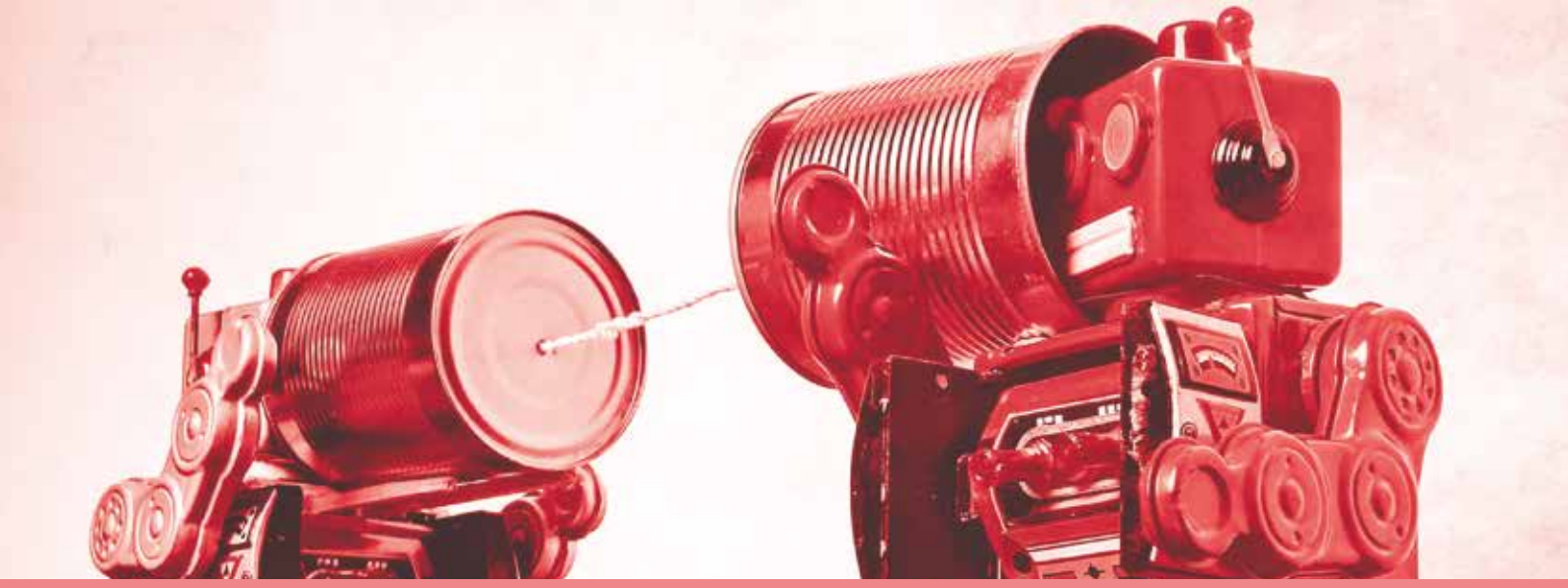

ICLG

The International Comparative Legal Guide to:

Telecoms, Media & Internet Laws & Regulations 2019

12th Edition

A practical cross-border insight into telecoms, media and internet laws and regulations

Published by Global Legal Group, with contributions from:

Arioli Law
Arnold & Porter
Ashurst Hong Kong
Attorneys-at-Law TRUST
Bagus Enrico & Partners
BEHRING
Bello, Gallardo, Bonequi y Garcia, S.C.
BTG Legal
Cairn Legal
CMS (UAE) LLP
D'LIGHT Law Group
Drew & Napier LLC
Fasken
Focaccia, Amaral, Pellon & Lamônica Advogados
Jingtian & Gongcheng
Kahale Abogados
Kalema Legal & Associates
Khaitan & Co
Mazanti-Andersen Korsø Jensen
MinterEllison
Monereo Meyer Abogados
Mori Hamada & Matsumoto
Nikolinakos – Lardas & Partners LLP
Pinsent Masons Germany LLP
Portolano Cavallo
Preiskel & Co LLP
Rato, Ling, Lei & Cortés – Advogados
RIAA Barker Gillette
Shearn Delamore & Co.
Tilleke & Gibbins
Ünsal Gündüz Attorneys at Law
Wilkinson Barker Knauer, LLP

MEF MOBILE ECOSYSTEM FORUM
glg global legal group

global legal group

Contributing Editor
Rob Bratby, Arnold & Porter

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Toni Hayward

Sub Editor
Amy Norton

Senior Editors
Suzie Levy
Caroline Collingwood

Chief Operating Officer
Dror Levy

Group Consulting Editor
Alan Falach

Publisher
Rory Smith

Published by
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

GLG Cover Design
F&F Studio Design

GLG Cover Image Source
iStockphoto

Printed by
Stephens & George
Print Group
November 2018

ISBN 978-1-912509-45-4
ISSN 2050-7607

Strategic Partners

General Chapters:

Country Question and Answer Chapters:

Chapter 3

Liable *vs.* Accountable: How Criminal Use of Online Platforms and Social Media poses Challenges to Intermediary Protection in India

Vikram Jeet Singh

Prashant Mara

BTG Legal

Abstract

The term "Cybercrime" feels particularly outdated nowadays. It is used to signify (comparatively) humdrum acts like online obscenity, identity theft, or financial malfeasance. Now, there is an argument that the Internet enables (or even abets) extreme cases of criminality, such as rioting, hate speech, terrorist recruitment, targeted fake news, illegal lobbying, and unprecedented thefts of personal data. A number of these cases involve online platforms and intermediaries (being used as primary tools for commission of crime), the new gatekeepers of the Internet.

Countries around the world are struggling to apply old legal paradigms to these new problems. The concept that an intermediary is only a neutral "pipeline" for information is no longer sacrosanct. Germany's new social media law makes the social media platform liable for the content they carry. The Indian Supreme Court and the Ministry of Electronics and Information Technology have repeatedly called for the regulation of intermediaries providing Internet platforms. In fact, the Supreme Court has in the past made intermediaries responsible for actively monitoring platforms, to ensure that they are compliant with child and women protection laws.

It is becoming evident that the old standard of intermediary liability will not survive the reality of the new Internet. In a country like India, where more than half a billion people have access to the Internet, these issues will be at the forefront of regulation in the near future. It is also important not to overlook the transformative potential of Internet access in India. Laws that indiscriminately inhibit the openness and accessibility of the Internet will benefit no one. It would be better if these laws were written in partnership with intermediaries, rather than being handed on from high with a flawed understanding of how the Internet works.

This chapter examines two questions in the context of growing calls for regulation in India:

Are we moving from a "did-not-know" standard to a "ought-to-have-known" standard, and to what extent is this practical?

Do we need a new hypothesis of intermediary liability, which is limited but varies with degrees of potential harm?

Evolution of Intermediary Protection "Safe Harbour"

"*The law should allow internet platforms to stay out of editorial decisions so that people can share and speak freely.*"

– Wikimedia Foundation

The United States dominates in a study of governance landscape for online intermediaries, as US law provides robust protections for speech, rooted in the First Amendment to the United States Constitution. This is coupled with the fact that most leading Internet companies are based in the US.

Tellingly, US law relating to intermediary protection evolved as a result of defamation cases. In *Cubby vs. CompuServe Inc.* (1991), a New York district court applied defamation liability laws to an Internet service provider hosting an online news forum.[1] CompuServe argued that it was a distributor, not a publisher, and therefore could not be liable without knowledge. The court noted that the requirement for a distributor to have knowledge of the contents of a publication, before liability can be imposed for distributing that publication, is deeply rooted in the US First Amendment. Since no specific facts were shown indicating that CompuServe knew or had reason to know of defamatory content, it was held to be not liable for such content.

An intermediary's knowledge was again at question in *Stratton Oakmont vs. Prodigy* (1995). This time, the New York State's Supreme Court established that the intermediary, Prodigy Services, who published a "*Money Talk*" bulletin board, clearly made decisions regarding content, and had "*uniquely arrogated to itself the role of determining what is proper for its members to post and read on its bulletin boards*".[2]

In 1996, the *Stratton* decision led the US Congress to pass Section 230 of the Communications Decency Act in order to protect Internet intermediaries from liability for third-party content. Section 230 states that "*No 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*". That is to say, online intermediaries that host or publish content are protected against a range of laws that might otherwise be used to hold them legally responsible for what others say and do.

Section 230 of the Communications Decency Act, 1996, was a seminal step; it has been called "*The Law that Gave Us the Modern Internet*".[3] Following the US' lead, a number of other jurisdictions have taken a pro-intermediary stance when providing for or interpreting safe harbour provisions.

Indian Laws on Intermediaries

India enacted its intermediary protection laws four years after the US, as part of its Information Technology Act, 2000. Section 79 of the Information Technology Act, 2000 ("**IT Act**"), provides intermediaries with qualified immunity from liability under all other laws. "*Intermediary*" is defined widely to mean "*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*".

The "*intermediary defense*" under Section 79 is available as long as intermediaries follow prescribed due diligence requirements and do not conspire, abet or aid an unlawful act. The protection under Section 79 lapses if an intermediary with "*actual knowledge*" of any content used to commit an unlawful act, or on being notified of such content by the Government, fails to remove or disable access to the unlawful material. The due diligence requirements to be observed by intermediaries under Section 79 are prescribed in the Information Technology (Intermediary Guidelines) Rules, 2011 ("**Intermediary Rules**"). The intermediary is required to publish rules and regulations, a privacy policy and a user agreement for access or usage of its computer resources.

In 2015, in *Shreya Singhal vs. Union of India*, the Supreme Court of India read down the term "actual knowledge", used in Section 79, to mean that the intermediary would be required to remove or disable access to unlawful material only upon receiving knowledge that a court order has been passed asking the intermediary to do so, or upon receiving notification from an appropriate government. This broadly follows the concept in Section 230 of not attributing knowledge or liability to an intermediary without good cause. It is interesting to note that the decision in *Shreya Singhal* was couched, in part, in terms of the fundamental right of free speech.

The Breakdown of the "Safe Harbour"

The principal of safe harbour for intermediaries has held for more than two decades, but is now increasingly questioned. This is a function of both time passing, and of the wider form this protection has taken. The Communications Decency Act, 1996, was enacted due to concerns over pornography on the Internet. US courts have since interpreted it expansively, granting broad immunity even from civil rights violations.[4]

The biggest challenge to the Intermediary's safe harbour rule has been from laws aiming to prevent online sex trafficking. In 2017, the Stop Enabling Sex Traffickers Act ("**SESTA**") amended the protection in Section 230. This Act specifies that provisions protecting providers from liability shall not limit civil action or criminal prosecution relating to sex trafficking of children or sex trafficking by force, fraud, or coercion.

In the EU, efforts are being made to compel intermediaries to combat hate speech on their platforms. A new German *Netzwerkdurchsetzungsgesetz* (an Act to Improve Enforcement of the Law in Social Networks) aims to do just that. It applies to all Internet platforms that enable users to share content. It requires such platforms to delete manifestly unlawful content within 24 hours of a complaint. This makes the platform liable to make such determination itself, within a very short period of time. Content that is not 'manifestly' unlawful can be deleted in a longer timeframe, within seven days.

The law relating to intermediaries evolved at a very different time (when online bulletin boards were the norm) to address a very different need (applying the publishers' liability for defamation standard to the Internet). The "*library vs. newspaper*" debate that dominated the '90s has lost relevance in an age where the Internet has replaced not just the library and the newspaper, but the post office, the television, the landline phone and the cinema. As developments in the US and the EU show, the safe harbour for intermediaries cannot be applied in all cases.

In India, the derogation from an absolute theory of intermediary liability has come from two sources: copyright protection laws; and public order offences.

Following the Supreme Court's decision in *Shreya Singhal*, the Delhi High Court in *MySpace Inc. vs. Super Cassettes Industries Ltd.*[5] seems to hold that in cases of copyright infringement, a court order is not necessary, and an intermediary must remove content upon receiving knowledge of the infringing works from the content owner. As such, it seems that the intermediary protection provided in the *MySpace* case was considerably less than the "*actual knowledge*" requirement under Section 79 of the IT Act, as read by *Shreya Singhal*.

The other challenge to intermediary protection has been the use of platforms in criminal activities. Incidents of lynching and mob violence have been reported from videos and messages circulated on the WhatsApp platform in India.[6] The Indian Government's Ministry of Electronics and Information Technology has taken up these matters with WhatsApp on at least two occasions, asking it to find effective solutions to the misuse of its platform.[7] Most worryingly for intermediaries such as WhatsApp, the Government has indicated that if they do not find such solutions, they are "*liable to be treated as abettors*" and "*face consequent legal action*". In the worst case scenario, this may mean that intermediaries are prosecuted as abettors under the Indian Penal Code.

Preserving the Safe Harbour

We seem to be living in the sunset of the traditional theory of intermediary protection. A blank-cheque approach to intermediary protection has led to a global backlash. Given the growing number of Internet users in India, the serious impact that intermediaries' passive role has on society and politics is coming under increasing scrutiny from regulators. It is more than likely that a regulatory alternative will emerge which will water down the overarching protections available to intermediaries.

The question, then, is what would this regulatory alternative be, and could intermediaries drive the discussion to an alternative that balances their liability, the freedom of speech of their users, and law enforcement requirements?

Possible ways forward have been shown by a combination of the German *Netzwerkdurchsetzungsgesetz*, and jurisprudence around copyright content removal. Intermediaries may have to take a proactive role in policing and removing certain kinds of content. So long as there is broad consensus on what these "high-risk" types of content are, intermediaries should be allowed to evolve an internal self-regulatory mechanism to track and address such content. Obvious examples are child-harming content, and material that incites violence, religious intolerance or enmity, etc. As noted in the German *Netzwerkdurchsetzungsgesetz*, such content should be banned/removed expeditiously within 12–24 hours. For content that is not obviously a part of such illegal categories, a longer process of adjudication/discussion can be specified. An example of the latter would be copyright violation.

In terms of process, it may be useful for intermediaries to come together and design a cross-platform format that can be used by users to report such illegal content. A growing body of such reports can then be used to analyse the trends of removal of content, and can slowly become the basis for any guidelines for self-regulation.

Such "increased" or "pro-active" diligence on the part of the intermediaries should be recognised in any future law as being sufficient a criterion to preserve the safe harbour defence. One-off "misses" in removing high-risk content should not impose

liability on intermediaries if they can demonstrate that a process was available. Admittedly, this will be a subjective determination, but as we have seen in the case of GDPR, some level of subjectivity and application of judgment has become unavoidable in the growing body of new legislation governing online behaviour.

Conclusions

Inaction on the issue of intermediary liability will not be an option for much longer. In the absence of a solution from the industry, governments and regulators may go for an extreme "banning" approach, or try to affix "criminal liability" on intermediaries. The Indian government has already referenced the criminal act of "abetting" in connection with WhatsApp. At the same time, the Indian Supreme Court has, in the *Prajwala* case, shown willingness to work with intermediaries to come up with solutions to online content problems. The choice may come down to intermediaries, in whether to work alongside regulators and evolve the next standard of intermediary liability, or to take up a reactive, defensive view to the regulations that are laid upon them.

Endnotes

1. 776 F. Supp. 135 (S.D.N.Y. 1991).
2. 1995 WL 323710.
3. https://www.theatlantic.com/business/archive/2013/09/the-law-that-gave-us-the-modern-internet-and-the-campaign-to-kill-it/279588/.
4. *The Overexpansion of the Communications Decency Act Safe Harbor*, Joey Ou, Hastings Communications and Entertainment Law Journal, 455 Volume 35 Number 3.
5. 2017 (69) PTC 1.
6. *Viral WhatsApp Messages Are Triggering Mob Killings In India*, July 18, 2018, Lauren Frayer, https://www.npr.org/2018/07/18/629731693/fake-news-turns-deadly-in-india.
7. The Ministry issued two press releases in this regard, on July 3, 2018 and on July 19, 2018.

Vikram Jeet Singh
BTG Legal
804 Lodha Supremus
Dr. E. Moses Road
Worli, Mumbai – 400018
India

Tel: +91 22 2482 0820
Email: vikram@btg-legal.com
URL: www.btg-legal.com

Vikram Jeet Singh is a partner in the Digital Business practice group and specialises in laws relating to digital payments, social media, online marketplaces and e-commerce.

Vikram has advised clients on acquiring entities in the digital payments space, acquiring card payment businesses through asset sales, interacting with regulators to implement online business models for his clients and managing related investigations and disputes.

As India counsel, Vikram has assisted his overseas technology clients in suits against the Indian Railways (in Lucknow District Courts) and in enforcing foreign arbitral awards against Indian counterparts (in the Delhi High Court). In addition, Vikram has independently assisted Indian subsidiaries of overseas companies in defending suits filed by ex-employees in local courts in Delhi.

Vikram qualified at the National Law School of India University, Bangalore. He has previously worked at Unilever India and at the Indian relationship firm of a leading US-headquartered firm.

Prashant Mara
BTG Legal
804 Lodha Supremus
Dr. E. Moses Road
Worli, Mumbai – 400018
India

Tel: +91 22 2482 0820
Email: prashant@btg-legal.com
URL: www.btg-legal.com

Prashant Mara is a commercial and regulatory lawyer with a focus on strategic investments and collaborations, compliance, procurement projects, investigation support and dispute management. He specialises in the technology, defence (with a focus on technology transfer and licensing) and industrials (with a focus on technology deployment) sectors.

Prashant was previously co-head of the India Group at Osborne Clarke and prior to that ran the India desk of a Franco-American firm in Paris. He started his career as in-house counsel in Infosys and managed their European legal operations.

Prashant is qualified to practise in India and read law at the National Law School of India University, Bangalore.

Current titles in the ICLG series include:

- Alternative Investment Funds
- Anti-Money Laundering
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Investigations
- Corporate Recovery & Insolvency
- Corporate Tax
- Cybersecurity
- Data Protection
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Financial Services Disputes
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Investor-State Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Investment Funds
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant

glg global legal group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: sales@glgroup.co.uk

www.iclg.co.uk