sflc.in

INTERMEDIARY LIABILITY 2.0

A SHIFTING PARADIGM

MARCH 2019

Intermediary Liability 2.0: A Shifting Paradigm

Published by: SFLC.in

SFLC.in
K-9, 2nd Floor, Birbal Road
Jangpura Extension
New Delhi – 110014
India

Email: mail@sflc.in
Website: https://www.sflc.in
Twitter: @SFLCin

Table of Contents

LIST OF CASES

LIST OF ABBREVIATIONS

Anr.	Another
v.	Versus
CrPC	Code of Criminal Procedure
Draft Rules	Draft Information Technology [Intermediaries Guidelines (Amendment) Rules], 2018
EU	European Union
Govt.	Government
HC	High Court
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and Communication Technologies
IP	Internet Protocol
IPC	Indian Penal Code
IT	Information Technology
LEA	Law Enforcement Agency
NGO	Non-Governmental Organization
OECD	Organization for Economic and Cultural Development
OHCHR	Office of the High Commissioner of Human Rights
Ors.	Others
SC	Supreme Court
SFLC.in	Software Freedom Law Centre, India
MeitY	Ministry of Electronics and Information Technology
UDHR	Universal Declaration of Human Rights
UK	United Kingdom
UN	United Nations
UNESCO	United Nations Educational Social and Cultural Organization
USA	United States of America
COAI	Cellular Operators Association of India
CCAOI	Cyber Cafe Association of India
FICCI	Federation of Indian Chambers of Commerce and Industry
ASSOCHAM	Associated Chambers of Commerce and Industry
NASSCOM	National Association of Software and Services Companies
AMCHAM	American Chamber of Commerce in India
ISPAI	Internet Service Providers Association of India
CII	Confederation of Indian Industry
IAMAI	Internet and Mobile Association of India

ACKNOWLEDGEMENTS

We express sincere gratitude to our knowledge partner Mishi Choudhary and Associates LLP without whose support, this report would not have been made possible. We also thank the intermediaries whose inputs provided valuable direction for our research. In addition, we are grateful to all who took time out of their busy schedules to participate in our events on intermediary liability and fake news.

CHAPTER I

INTRODUCTION

When Internet platforms were growing their business in the United States, they were considered bastions of free speech and were given 'safe-harbour' against third party content to promote innovation on the condition that they will self regulate their platforms for illegal content.[1] Over time, these companies acquired millions of users around the world and began centralizing power by subsuming smaller businesses within themselves.[2] For example, Facebook had acquired both WhatsApp and Instagram by 2014 to consolidate its business into a social media and private communications behemoth.[3]

As these platforms grew, it became increasingly difficult for them to self-regulate the large volume of content flowing through their pipelines. The misuse of data available on platforms, coupled with the growing menace of disinformation and misinformation online, increasing calls for imposition of greater liability on intermediaries for third party copyright infringement, access and assistance to law enforcement agencies and the rampant harassment and abuse of women and other vulnerable groups have highlighted the failures of these tech companies in regulating their channels. Not only did companies fail to police their platforms, they developed business models that directly conflicted with any such objective. Their business of advertisement sales came to be based on a continuous flow of behaviour data acquired by monitoring users of their platforms. The profitability of this business depends on maximizing the amount of time users spend on a platform. So, the goal became algorithmic recommendation of arresting content that sticks eyeballs to the platform and causes behaviour that can be used to profile readers for advertisers. Thus the real objective of the system is almost directly in opposition to the perceived social good the platforms are supposed to further.

By monitoring users' reading and behaviour,

(1) Section 230 of the Communications Decency Act, ELECTRONIC FRONTIER FOUNDATION, (Mar. 08, 2019, 10:04 AM), https://www.eff.org/issues/cda230

(2) Google has been steadily consolidating its Internet business by making strategic acquisitions - Matt Reynolds, If you can't build it, buy it: Google's biggest acquisitions mapped, WIRED, (Mar. 08, 2019, 10:0 AM), https://www.wired.co.uk/article/google-acquisitions-data-visualisation-infoporn-waze-youtube-android

(3) Joe Nocera, Why WhatsApp Is No Threat to Facebook's Dominance, BLOOMBERG OPINION, (Mar. 06, 2019, 11:04 AM), https://www.bloomberg.com/opinion/articles/2018-05-04/whatsapp-and-instagram-are-no-threat-to-facebook-s-dominance

the platform companies ceased to be the neutral conduit for "user-generated content" that justified their safe-harbour immunity in the first place. Collecting and analyzing all their users' behaviour, and aggregating what they captured themselves with all the other personally-related information they could buy, the platforms ceased to perform the task of democratizing expression: that became a by-product of their real effort, which was — in the phrase originally adopted by the US national security agencies — Total Information Awareness.

The platforms that were granted safe harbour protections were expected to police their platforms but have failed miserably to do so. Victims of online abuse, harassment have no leverage to insist that platforms respond to their complaints. Companies have failed to establish mechanisms to address complaints swiftly and continue to play the game of "Lexi Loci Server" claiming they only have a "sales offices" in India. On the other hand, governments more often than not have used this failure, ambiguity and secrecy to enact overtly broad legislation that facilitate censorship by proxy and stifle innovation.

Countries around the world have called for greater regulation of their activities. In 2017 Germany enacted a law for the takedown of illegal content. As of the date of publication of this report in 2019, an anti-encryption law has emerged in Australia, the proposed EU copyright directive requires proactive content filtering, and the draft EU terrorist content regulation requires takedowns within an hour of content being flagged.

Internet platforms have systematically failed to protect user rights in certain, particularly egregious cases. In India, per certain estimates, 33 people were killed in 69 incidents of mob violence between January 2017 and July 2018, their "lynchings" being linked to messages or "fake news" being spread on WhatsApp, the Facebook-owned messaging platform.[4]

In 2018, Facebook was used to spread anti-Rohingya propaganda for inciting murders, rapes and the largest forced human migration in recent history.[5] Most of the 18 million Internet users in Myanmar consider Facebook to be the Internet. It was reported that members of the Myanmar military were the prime operatives behind the systematic campaign, exploiting the wide reach of Facebook.[6] The social media platform was accused of doing little to prevent the harmful content from proliferating on its platform. Even though, Facebook eventually deactivated the accounts of the military personnel, millions of sham accounts went undetected.[7]

In the United States, the role of platforms like Facebook and Twitter in the 2016 presidential election has given way to society wide skepticism about tech companies and invited a kind of backlash that was unimaginable a few years ago.[8] Senators Mark Warner (D-VA) and Amy Klobuchar (D-MN) introduced the Honest Ads Act following the use of Facebook advertisements by Russian provocateurs, that would require platforms to make "reasonable efforts" to bar foreign nationals from purchasing certain categories of political advertisements during campaign.[9]

During the media blitzkrieg following the Cambridge Analytica scandal and before his US Congressional hearing, Mr. Zuckerberg in an interview to CNN said, "I actually am not sure we shouldn't be regulated. I think, in general, tech-

---

(4) IndiaSpend, Child-lifting rumours caused 69 mob attacks, 33 deaths in last 18 months, BUSINESS STANDARD, (Mar. 06, 2019, 12:30 PM), https://www.business-standard.com/article/current-affairs/69-mob-attacks-on-child-lifting-rumours-since-jan-17-only-one-before-that-118070900081_1.html

(5) Paul Mozur, A Genocide Incited on Facebook, With Posts From Myanmar's Military, NEW YORK TIMES, (Nov. 06, 2018, 12:30 PM), https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html

(6) Id.

(7) Id.

(8) Russia 'meddled in all big social media' around US election, BRITISH BROADCASTING CORPORATION-BBC, (Jan. 09, 2019, 12:50 PM), https://www.bbc.com/news/technology-46590890

(9) Heather Timmons and Hanna Kozlowska, Facebook's quiet battle to kill the first transparency law for online political ads, QUARTZ, (Sep. 06, 2018, 1:30 PM), https://qz.com/1235363/mark-zuckerberg-and-facebooks-battle-to-kill-the-honest-ads-act/

nology is an increasingly important trend in the world. I think the question is more what is the right regulation rather than 'yes or no' should we be regulated?"[10]

Intermediary liability – the focus of this report – illustrates how lawmakers were forced by the Internet to conceptualize and implement new approaches to an old legal construct i.e. vicarious liability. Intermediaries like blogging platforms, discussion boards and social media sites that offer platforms for users to publish self-generated content, search engines that index and provide access to user-generated content, online shopping sites that allow users to trade in products/services and so on raised the question: who is to be held liable in the event that some products, services, or content hosted by these intermediaries were found to be unlawful?

The answer to this question has been different in different jurisdictions.
While some jurisdictions like Thailand and China hold intermediaries strictly liable for user-generated content, others like the European Union and the United States grant them conditional immunity from liability, where compliance with certain conditions specified under relevant laws immunizes intermediaries from the consequences of unlawful user-generated content. India's own Information Technology Act, 2000 was amended in 2008 to introduce such a safe-harbour regime, and the Information Technology (Intermediaries Guidelines Rules), 2011 specified certain due-diligence criteria that intermediaries were to observe in order to qualify for immunity. The initial version of this regime was plagued by several problems including ambiguity in prohibited content and forced adjudication by intermediaries, but much of these problems were resolved by a historic judgment of the Supreme Court of India in 2015 in the matter of *Shreya Singhal v. Union of India*. Subsequently, on December 24, 2018, the Ministry of Electronics and Information Technology issued Draft Rules proposing to amend the 2011 Rules to include prescriptive obligations on the intermediary such as enabling traceability of the originator of the information, deploying automated tools for proactive monitoring of content and incorporation under the Companies Act. The reason for this, as provided by MeitY was "Misuse of Social Media and spreading Fake News".

In India, the regulation of intermediaries are spread out across various laws and sub-legislations. Apart from the IT Act, India's copyright law institutes a notice-and-takedown regime for intermediaries. Sector specific regulation such as data localisation requirements as per the rules of the Reserve Bank of India for fintech players and license requirements for telecom and Internet service providers also apply. In addition to this, the courts have interpreted law with substantial variance, making the intermediary liability landscape of India complicated enough to cause confusion to tech companies.

Due to the lapse in judgment of intermediary platforms in various situations as highlighted above, sovereign states around the world are demanding more accountability from them for user generated content on their portals. Nation states while imposing regulations on Internet companies must be mindful that such rules should not be over-broad resulting in hampering basic digital rights such as privacy and free speech in the online word.

SFLC.in had published a report in 2014 titled "The Information Technology (Intermediaries Guidelines) Rules, 2011: An Analysis". The report discussed the contemporary intermediary liability regime in India, highlighted its shortcomings and presented takeaways from stakeholder consultations that were organized in four major cities, pointed out relevant existing research, and proposed a set of principles that should guide an ideal intermediary liability regime. The present report is intended as a follow-up to the earlier report, necessitated in part by significant changes introduced to India's intermediary liability regime through judicial pronouncements and the proposed amendment to the 2011 Rules.

---

(10) Rob McLean and Danielle Wiener-Bronner, Mark Zuckerberg in his own words: The CNN interview, CNN MONEY, (Sep. 06, 2018, 1;47 PM), https://money.cnn.com/2018/03/21/technology/mark-zuckerberg-cnn-interview-transcript/index.html

This report will briefly go over the current state of intermediary liability laws in the country, examine some notable litigations that have served to better define the contours of this legal framework, highlight ongoing litigations that may significantly impact India's intermediary liability regime in the future, evaluate the present legal framework for compliance with applicable international standards, and provide glimpses into legal frameworks and case studies from other jurisdictions including in areas such as right to be forgotten that are indirectly connected to intermediary liability but bear significant implications for it nonetheless.

This report does not claim to offer simple solutions for a complicated problem. It hopes to offer suggestions that contain a critical way of thinking about the proposed legislative and regulatory reforms instead of adopting an ineffective mix of overtly broad yet ineffective regulations that facilitate censorship by proxy without addressing the notorious problem of "fake news" and disinformation.

Disinformation is a vast topic in itself, and this report has looked at it mainly from the point of view of intermediary liability.

CHAPTER II

WHAT IS INTERMEDIARY LIABILITY?

2.1 Defining an intermediary

An intermediary in the context of the Internet can be understood as an entity that acts as a facilitator of the flow of data across the vast and complex synapses of the Internet. While the actual functions of intermediaries are dynamic and often not clear-cut, they can broadly be seen as falling into one of two categories i.e. *conduits* for data traveling between nodes of the Internet, *hosts* for such data.[11] An Internet intermediary could therefore refer to Telecom Service Providers (TSP) that supply network infrastructure like optic-fiber cables and spectrum bandwidth over which Internet data is transmitted, Internet Service Providers (ISP) that utilize this infrastructure to offer Internet connectivity to the public, web-hosting platforms that provide servers on which Internet data is stored, search engines that sort through and index petabytes of data for easy retrieval, and the myriad online services that provide ways for end-users to leverage the power of the Internet for the efficient conduct of activities like commerce, governance, education, entertainment, and social networking to name a few. In other words, intermediaries play very crucial roles in the functioning of the Internet. Owing to the complex and diverse nature of functions performed by intermediaries, significant variations can be seen in global and national efforts at formally defining the term. The Organization for Economic Co-operation and Development (OECD) in April 2010 proposed that "Internet intermediaries" be defined as follows: [12]

"Internet intermediaries bring together or facilitate transactions between third parties on the Internet. They give access to, host, transmit and index content, products and services originated by third parties on the Internet or provide Internet-based services to third parties."

The OECD also identified the following as falling within the scope of this definition, though it was also careful to leave room for future expansion: ISPs, data processing and web-hosting providers, search engines, e-commerce platforms, Internet payment systems, and participative networking

---

(11) APC, *Frequently asked questions on Internet Intermediary Liability,* ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS, (Feb. 06, 2018, 2:50 PM) https://www.apc.org/en/pubs/apc%E2%80%99s-frequently-asked-questions-Internet-intermed

(12) OECD, *Definitions*, 9, THE ECONOMIC AND SOCIAL ROLE OF INTERMEDIARIES 2010,https://www.oecd.org/Internet/ieconomy/44949023.pdf

platforms. This definition was also cited by the United Nations Educational, Scientific and Cultural Organization (UNESCO) in a 2014 report on Internet freedoms.[13]

Some national jurisdictions on the other hand, have chosen to not attempt defining the term "intermediary" as such in relevant laws. Instead, broader alternate terms like "information society services"[14] and "interactive computer services" [15] are employed, and intermediary regulations are incorporated into law without referencing the term "intermediary".

The above being said, this report examines intermediary liability primarily in the context of Indian law. As such, the best place to look to understand the term "intermediary" for the purposes of this report is the IT Act – specifically Section 2(1)(w), which defines the term in some detail.

Section 2(1)(w) reads:
"Intermediary, with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, Internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes."

According to Section 2(1)(w) of the IT Act therefore, an intermediary is any person who receives, stores or transmits an electronic record [16] on behalf of another person or provides any service with respect to that record. [17] The Section then clarifies that the term includes telecom service providers, network service providers, Internet service providers, web hosting service providers, search engines, online payment sites, online auction sites, online marketplaces and cyber cafes. [18] This list is non-exhaustive and Section 2(1)(w) also covers entities such as social media websites, blogging platforms, message boards, consumer review websites and so on. In other words, virtually any website that features user-generated content and a large number of Internet service providers fall within the definition of an intermediary under Section 2(1)(w) of the IT Act.

2.2 User-generated content and liability

"Intermediary liability", to put it simply, refers to the extent of liability that an intermediary stands to incur due to the non-permissibility under law of content they deal in. Seeing how intermediaries neither create nor modify content, the predominant consensus has been that it would be inequitable to hold them strictly accountable for unlawful user-generated content. Users of intermediary services are the true content creators and as such, it has generally been felt that they should be the ones made to answer for the illegality of content hosted or transmitted on intermediary platforms unless intermediaries have meaningful degrees of editorial control. However, some jurisdictions such as China and Thailand have opted to see things differently and maintained that it is the responsibility of

---

(13) R. MacKinnon, E. Hickok, A. Bar, H. Lim, *Fostering Freedom Online – The Role of Internet Intermediaries,* UNESCO Series on Internet Freedoms, 2014, (Sep. 26, 2017, 2:50 PM), http://unesdoc.unesco.org/images/0023/002311/231162e.pdf

(14) Directive (EU) 2015/1535 of the European Parliament and of the Council, laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1551937833098&uri=CELEX:32015L1535

(15) 47 USC S.230 (f)(2), The term "interactive computer service" means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.

(16) Information Technology Act 2000 Section 2(t), An *"electronic record"* is *"data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche"*. Section 2(o) 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 formalized 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"*.

(17) Information Technology Act 2000 Section 2(w)

(18) Id.

platform providers i.e. intermediaries to ensure that the content they host or transmit remains within the confines of legal permissibility.

Based on these divergent viewpoints, three broad models of intermediary liability have emerged globally, as pointed out by Article 19 in their 2013 report titled *"Internet Intermediaries: Dilemma of Liability"*.[19] These are:

(1) The strict liability model: Intermediaries are held unconditionally liable for user-generated content. Intermediaries are effectively required to monitor content in order to comply with the law; if they fail to do so, they face a variety of sanctions, including the withdrawal of their business license and/or criminal penalties. Examples include Thailand and China.

(2) The safe-harbour model: Intermediaries are given conditional immunity from liability arising out of user-generated content i.e. if they comply with certain requirements laid out under law. This model can be further divided into:

(a) *The vertical model:* Liability is determined according to the type of content at issue. No distinctions are made as to the type of service provided by intermediaries e.g. hosting vs. transmitting.

(b) *The horizontal model:* Liability is determined according to the kind of function performed by the intermediary. Intermediaries acting only as a transmitter of content may thus be exempted unconditionally from liability whereas those acting as hosts may be held to more stringent standards. The latter may forfeit immunity if they do not expeditiously remove unlawful content on being notified.

The safe-harbour model is also characterized by the existence of "notice-and-takedown" processes, which are legally prescribed procedures that clearly outline how content takedown requests must be received and processed by intermediaries. Intermediaries may further be encouraged to institute some form of technology-based or self-regulatory content filters so as to prevent the publication of unlawful content. The EU e-commerce Directive, US Digital Millennium Copyright Act and the Indian IT Act are legislations that employ this model of intermediary regulation.

(3) The broad immunity model: Intermediaries are given broad, at times conditional, immunity from liability arising out of user-generated content. Notably, intermediaries are also expressly excluded from any obligation to monitor for unlawful content. This model treats intermediaries as messengers who merely transmit content on behalf of users, rather than publishers of content. Section 230 of the Communications Decency Act is an example of this model.

Regardless of the model, almost all regulatory regimes overseeing Internet intermediaries obligate intermediaries to remove unlawful content from their platforms upon being asked to do so in accordance to applicable legal procedures. This, coupled with the fact that availability of immunity from liability is contingent in some regulatory regimes on expeditious compliance with takedown requests, means that regulators and intermediaries alike must be mindful of the impact of their actions on freedom of expression, which is a fundamental human right recognized under almost all major national and international jurisdictions. Regulators that impose ambiguous content limitations or ask intermediaries to remove content based on their own judgement while running the risk of forfeiting safe-harbour protection for non-removal of content, as well as intermediaries that over-comply with takedown requests will adversely impact freedom of expression. Google's transparency reports shows that there has been a sharp increase in the number of content takedown requests received from governments in recent times. While Google received 1,031 such requests in the second-half of 2009, this number climbed to 15,961 in the second half of 2016, representing a fifteen-fold increase.[20] The latest report reveals that 25,534

(19) Article 19, *Internet Intermediaries: basic facts,* 7 INTERNET INTERMEDIARIES: DILEMMA OF LIABILITY 2013, https://www.article19.org/data/files/Intermediaries_ENGLISH.pdf

(20) Google,Government Requests to Remove Content, Google Transparency Report, GOOGLE (Feb. 26, 2019, 2:50 PM), https://transparencyreport.google.com/government-removals/overview?hl=en

requests were received in the first half of 2018 itself.[21] According to this report, national security is the most cited reason for takedown requests with 11,430 and 17,999 requests in the years 2016 and 2017 respectively.[22] This is followed by defamation with an increase from 3,440 to 4,257 requests in years 2016 to 2017.[23] Takedown requests on the basis of 'Privacy and Security' have also increased from 2404 to 2497 requests in the years 2016 to 2017.[24]

(21) Id.
(22) Id.
(23) Id.
(24) Id.

CHAPTER III

The Intermediary Liability Regime in India

3.1 Enlarging the Scope of Safe-Harbour Protection

The Indian Government enacted the IT Act[25] to provide legal recognition to e-commerce, to facilitate electronic filing of documents with government agencies and amend other existing laws like the Indian Penal Code, 1860 and the Indian Evidence Act, 1872. This was based on the UN General Assembly adopting the Model Law on Electronic Commerce issued by the United Nations Commission on International Trade Law,[26] to which India was a signatory. According to the Statement of Objects and Reasons of the IT Act, *"There is a need for bringing in suitable amendments in the existing laws in our country to facilitate e-commerce. It is, therefore, proposed to provide for legal recognition of electronic records and digital signatures."*

At the time the IT Act was enacted, the definition of the term 'intermediary' was as follows:

Section 2(1)(w):
"intermediary" 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.

Section 79 is currently the provision that guarantees safe-harbour protection to intermediaries for third party content. Section 79 of the original Act only protected network service providers[27] from liability arising from third party content, if they proved absence of knowledge; or application of positive application of due diligence on their part to prevent commission of an offence/ contravention.[28]

---

(25) The IT Act came into force in India on 17 October, 2000.
(26) General Assembly of the UN, resolution A/RES/51/162 dated January 30, 1997.
(27) According to the previous Section 79 of the IT Act, network service providers meant - 'intermediaries' as defined under the Act.
(28) Sec. 79 - *Network service providers not to be liable in certain cases:*
For the removal of doubts, 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.

Subsequently, an amendment to the IT Act in 2008[29] ("the IT Amendment Act") made substantial changes to Section 79 (the safe-harbour provision) and the definition of intermediaries. One of the triggers for amending the IT Act in 2008, specifically for widening the protection given to intermediaries, was the MMS scandal affecting Baazee.com (at that time, a wholly owned subsidiary of Ebay Inc. USA). In this case, an MMS clip was listed on Baazee.com (an e-commerce website) which contained sexually explicit content which was being offered for sale on the website. For selling of such content on its website, Avnish Bajaj, the then Managing Director of Baazee.com. was arrested and criminally charged with provisions under the Indian Penal Code, 1860 ("the IPC") and the IT Act, which dealt with acts of obscenity. In a petition challenging the criminal charges against him, the Delhi High Court in *Avnish Bajaj v. State*[30] held that a prima facie case for obscenity may be made against Baazee.com. It cannot be made against Avnish Bajaj for provisions under the IPC, but he may be charged for publishing of obscene content in electronic form as per Section 67 of the IT Act[31] (it is important to note that Baazee.com was not arraigned in the case as an accused). The court in its judgment had stated that owners or operators of websites that offer space for listings might have to employ content filters to prove that they did not knowingly permit the use of their website for pornographic material.[32] On an appeal made by Avnish Bajaj against the charge under Section 67 of the IT Act, the Supreme Court of India in the year 2012,[33] quashed the proceedings against him on the ground that prosecution of the Managing Director could not go ahead without arraigning the company as an accused party. Drawing parallels between the Negotiable Instruments Act, 1881 and the IT Act in terms of offence by companies and the consequent liability of its officers, the court held that vicarious liability will only arise when the company is arraigned as an accused party.[34]

The IT Amendment Act enlarged the definition of the word 'intermediary'[35] to service providers like telecom service providers, Internet service providers, search engines, online marketplaces and even cyber cafes. It also widened the safe-harbour protection given to these intermediaries under Section 79[36] from only network service providers to all intermediaries and protected intermediaries from all unlawful acts rather than offences and contraventions covered under the IT Act itself. This new provision adopted a function based approach, wherein if the intermediary - (a) only provided access to a communication system for information made available by third parties, which is transmitted or temporarily stored/ hosted; and (b) it did not initiate the transmission, select the receiver and select/ modify the information, then it could claim protection under this provision for content made available by third parties (user generated content).

Explanation.—For the purposes of this section, —
(a) "network service provider" means an intermediary;
(b) "third party information" means any information dealt with by a network service provider in his capacity as an intermediary

(29) The Information Technology (Amendment) Act, 2008 came into force on 27 October, 2009 - https://meity.gov.in/writereaddata/files/act301009_0.pdf and the amendment act can be accessed here: https://meity.gov.in/writereaddata/files/it_amendment_act2008%20%281%29_0.pdf.

(30) Avnish Bajaj v. State, 150 (2008) DLT 769

(31) Section 67 of the then IT Act: Publishing of information which is obscene in electronic form - Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees.

(32) Avnish Bajaj v. State, 150 (2008) DLT 769

(33) Aneeta Hada v. Godfather Travels and Tours Pvt. Ltd, AIR 2012 SC 2795

(34) Avnish Bajaj v. State, 150 (2008) DLT 769

(35) Section 2(1)(w) of the IT Act.

(36) Section 79 of the IT Act.

The amended provision made this safe-harbour protection available to intermediaries based on certain conditions:

(I) Observance of due diligence and certain guidelines issued by the Central Government;

(II) Not conspiring, abetting, aiding or inducing the commission of the unlawful act; and

(III) Upon receiving 'actual knowledge' or being notified by the government, taking down unlawful content.

In the Report of the Expert Committee, set up by the Ministry of Information and Technology in 2005 to recommend changes to the IT Act, the rationale for amending the safe-harbour provision i.e. Section 79 was explained as to bring it in line with the EU's Directive on e-commerce (2000/31/EC).

3.2 'Due Diligence' Guidelines for Attaining Safe-Harbour

After the amendment to the IT Act in 2008, which incorporated the 'due-diligence' requirement for intermediaries for claiming safe-harbour, the Government of India on 11th April, 2011, issued the Information Technology (Intermediaries Guidelines) Rules, 2011[37] ("the Intermediaries Guidelines"). The Intermediaries Guidelines, inter alia, brought in the following conditions, which all intermediaries had to adhere to for their safe-harbour protection:[38]

(a) Publishing rules/regulations; privacy policies; user agreements;

(b) Terms and conditions to specify prohibited content- grossly harmful, harms minors, infringes intellectual property rights, contains virus (among other things)[39]

(c) A strict notice and takedown process;

(d) Assistance to government agencies for law enforcement;

(e) A duty to report cyber security incidents to the government; and

(f) Appointment and notification of a grievance officer.

According to the thirty-first report of the Parliamentary Committee on Subordinate Legislation,[40] which studied the Intermediaries Guidelines, among other delegated legislation notified by the Indian Government under the IT Act, there were a number of 'infirmities' with the Intermediaries Guidelines, the report identified them as:

(a) Ambiguous and Vague Terms: the committee recommended that to remove such ambiguity, terms which are borrowed from other laws shall be incorporated within the guidelines and undefined terms shall be defined and inserted into the text.

(b) Removal of Content by Intermediaries: the committee recommended that there is a need for clarity on the notice and takedown process and there should be safeguards to protect against any abuse during such process.

(c) Reconstitution of the CRAC - the Cyber Regulations Advisory Committee: the committee recommended that the CRAC must be reconstituted. It found that the CRAC had met twice since the enactment of the IT Act in the year 2000. According to the committee, MeitY would benefit from the advise of the CRAC and it should incorporate such members who represent the interests of the principally affected and who have special knowledge of the subject matter.

---

(37) The Intermediaries Guidelines Rules, http://dispur.nic.in/itact/it-intermediaries-guidelines-rules-2011.pdf

(38) To refer to the entire text of the Intermediaries Guidelines, kindly refer to https://www.wipo.int/edocs/lexdocs/laws/en/in/in099en.pdf

(39) For a full list of prohibited content, refer to Rule 3(2) of the Intermediary Guidelines available at https://www.wipo.int/edocs/lexdocs/laws/en/in/in099en.pdf

(40) The Report of the Committee, https://sflc.in/report-committee-subordinate-legislation-intermediaries-rules-tabled (SFLC.in had deposed before the committee highlighting its concerns with various provisions of the Intermediaries Guidelines).

Unfortunately, none of the recommendations made by the Committee on Subordinate Legislation were incorporated by the government either at the time of such consultation or subsequently.

3.3 Narrowing the scope of 'actual knowledge'

In a batch of writ petitions filed before the Supreme Court of India starting from 2012, a number of provisions of the IT Act were challenged - Section 66A (punishment for sending offensive messages), 69A (power to block websites) and 79 (safe-harbour provision) for severely affecting the fundamental right of free speech and expression as guaranteed under Article 19(1)(a) of the Constitution of India. This case - *Shreya Singhal v. Union of India*[41] which is otherwise popularly known as the *Shreya Singhal* judgment, struck down Section 66A of the IT Act as unconstitutional for having a chilling effect on free speech, (Section 66A[42] provided for punishment for sending offensive messages through communication services. It created criminal liability for sending information which was grossly offensive, inconvenient, insulting, dangerous etc.)

This was a landmark judgment in the Supreme Court's jurisprudence as for the first time the court recognized the Indian citizen's free speech rights over the Internet and struck down a draconian provision from the IT Act. As India's Constitution provides for 'reasonable restrictions' on free speech in certain circumstances [as per Article 19(2) of the Constitution],[43] the court in Shreya Singhal tried to read in the elements of Article 19(2) into Section 66A but failed to do so.

On the issue of intermediary liability, the Supreme Court read down Section 79 and held that the 'actual knowledge' requirement for an intermediary to take down content has to be read to mean either an intimation in the form of a court order or on being notified by the government and such requests must be restricted to the limitation listed by Article 19(2) of the Constitution. The court similarly read down the 'actual knowledge' requirement from the Intermediaries Guidelines which operationalised the notice and takedown mechanism under law -

"119. (c) Section 79 is valid subject to Section 79(3)(b) being read down to mean that an intermediary upon receiving actual knowledge from a court order or on being notified by the appropriate government or its agency that unlawful acts relatable to Article 19(2) are going to be committed then fails to expeditiously remove or disable access to such material. Similarly, the Information Technology "Intermediary Guidelines" Rules, 2011 are valid subject to Rule 3 sub-rule (4) being read down in the same manner as indicated in the judgment."

This marked a significant change in the intermediary liability regime in India, as previously any person could request intermediaries to take down content, if they felt it was unlawful. The law also placed intermediaries in a precarious position to adjudge the legality of content on their platforms, which directly conflicted with their status of being mere functionaries. In fact, the Supreme Court in Shreya Singhal acknowledged that intermediaries like Google and Facebook would have to act upon millions of requests for takedowns, making them the adjudicators as to which requests were legitimate according to law.[44]

The following inferences can be drawn to broadly sum-up India's Intermediary Liability law:

(a) Intermediaries need to fulfill the conditions under Section 79 of the IT Act as discussed above (conditional safe-harbour);

(b) Intermediaries are required to comply with all requirements listed under the Intermediaries Guidelines (due diligence rules); and

---

(41) Shreya Singhal v. Union of India, (2015) 5 SCC 1]

(42) For the entire text of the erstwhile Section 66A, kindly refer to Annexure

(43) Article 19(2) of the Indian Constitution places reasonable restrictions on free speech in the interests of - sovereignty and integrity of India, security of the state, friendly relations with foreign states, public order, decency or morality, contempt of court, defamation, or incitement to an offence.

(44) Para. 117 of the Shreya Singhal judgment

(c) Intermediaries, other than enforcing their own terms and conditions and privacy policies, are liable to take down content from their platforms only when notified by a court or an authorised government agency[45] and that too for matters listed under Article 19(2) of the Constitution (the actual knowledge requirement).

3.4 Proposed Amendment to Intermediaries Guidelines

On 24th December, 2018, MeitY released the Draft Information Technology [Intermediaries Guidelines (Amendment) Rules], 2018 ("the Draft Rules") to amend the existing Intermediaries Guidelines. These Draft Rules sought to introduce requirements on intermediaries like - tracing out of originator of information for assistance to law enforcement, deployment of automated tools for proactive filtering of unlawful content, takedown of illegal content within 24-hours, and mandatory incorporation of companies having 5 million + users in India (among other things).[46]

In a press note issued by MeitY[47] alongside the Draft Rules, it has been mentioned that social network platforms are required to follow due diligence as provided in Section 79 of the IT Act and the Rules notified therein, subject to the import of Article 19(2) of the Constitution, they have to ensure that their platforms are not used to commit and provoke terrorism, extremism, violence and crime. The press note also states that instances of misuse of social media platforms by criminals and anti-national elements have brought new challenges to law enforcement agencies, such as inducement for recruitment of terrorists, circulation of obscene content, spread of disharmony, incitement of violence, public order, fake news etc. The press note points to fake news/ rumours being circulated on WhatsApp and other social media platforms for various mob-lynching incidents reported across India in the last year. As MeitY has not issued any other official statement behind their intent in revising the intermediaries guidelines under the IT Act, the Draft Rules need to be read in conjunction with the press note for a critical examination of the proposed changes therein.

MeitY invited comments on the Draft Rules and received responses from around 150 stakeholders, a number of them expressing their concerns around the proposed guidelines for their capacity to severely affect free speech and privacy rights of citizens online.[48]

Key Issues with the Draft Rules

(A) The Traceability Requirement: Rule 3(5) of the Draft Rules requires intermediaries to enable the tracing out of originator of information on their platforms as may be required by authorised government agencies. The most concerning aspect of this requirement is how it will affect intermediaries like WhatsApp and Signal who provide personal communication services which are end-to-end encrypted[49] i.e. wherein even the service provider does not have access to the content of messages/ information which flows through their platform. Introducing a traceability requirement for end-to-end encrypted services will lead to breaking of such encryption and thus compromising the privacy of individuals making use of such services for their private communication. In August of 2017, a nine-judge bench of the Supreme Court in *KS Puttaswamy v. UOI* ("the Pri-

---

(45) As held by the Supreme Court of India in *Shreya Singhal*

(46) To refer to the entire text of the Draft Rules, see https://meity.gov.in/writereaddata/files/Draft_Intermediary_Amendment_24122018.pdf

(47) The press note issued by MeitY, http://pib.nic.in/newsite/PrintRelease.aspx?relid=186770

(48) SFLC.in participated in the public consultation and its comments and counter-comments to MeitY on the Draft Rules can be read here - https://sflc.in/our-comments-meity-draft-intermediaries-guidelines-amendment-rules-2018 and here - https://sflc.in/our-counter-comments-meity-draft-intermediaries-guidelines-amendment-rules-2018

(49) Explanation of the end-to-end encryption used by WhatsApp on its service, WHATSAPP (Nov 10, 2018, 11AM), https://faq.whatsapp.com/en/android/28030015/

vacy Judgment")[50], held the right to privacy[51] as a fundamental right guaranteed under the Constitution of India.[52]

(B) Proactive Filtering of Content: Rule 3(9) of the Draft Rules requires intermediaries to deploy automated tools for proactive filtering of unlawful content on their platforms. Online intermediaries are considered channels of distribution that play a merely neutral, technical and non-adjudicatory role. This Rule requires intermediaries to scrutinize user generated content and determine its legality - a task which must be undertaken by the judiciary considering that there are no clear standards of what is 'unlawful'. This provision of proactive content filtering is against the judgment in *Shreya Singhal* (as discussed above), where in the Supreme Court of India had held that intermediaries are neutral platforms that do not need to exercise their own judgment to decide what constitutes legitimate content.

Automated moderation systems that are in use today rely on keyword tagging which is then followed by human review. Even the most advanced automated systems cannot, at the moment, replace human moderators in terms of accuracy and efficiency. This is mainly because artificial intelligence is currently not mature enough to understand the nuances of human communication such as sarcasm and irony.[53] It should also be noted that global communication is influenced by cultural differences and overtones which an effective system of content moderation has to adapt to. Given the amateurish stage at which AI is at the moment, it may be short sighted to rely on this technology.

As societies evolve and change, so does the definition of "grossly harmful / offensive content". This implies that algorithms have to constantly understand nuanced social and cultural context that varies across regions. Research on AI has not yet produced any significant sets of data for this kind of understanding. The immediate result of using automated tools will be an increase in content takedowns and account suspensions which in turn will lead to over-censorship as has been seen around the world. Legitimate users (content creators) including journalists, human rights activists and dissidents will have their speech censored on a regular basis.

YouTube's "Content ID" system for detecting content that infringes copyright has been deemed notorious for over-censoring innocent material. Use of AI without human intervention for detecting hate speech, misinformation, disinformation, trolling, etc which is even more nuanced than identifying copyrighted material will be catastrophic for freedom of speech and expression on the Internet.

The key limitations of natural language processing tools are:[54]

(1) Natural language processing ("NLP") tools perform best when they are trained and applied in specific domains, and cannot necessarily be applied with the same reliability across different contexts;

(2) Decisions based on automated social media content analysis risk further marginalizing and disproportionately censoring groups that already face discrimination. NLP tools can amplify social bias reflected in language and are likely to have lower accuracy for minority groups who are under-represented in training data;

---

(50) WP (Civil) No. 494 of 2012

(51) The Supreme Court read in informational and communicational privacy as facets of the larger right to privacy in K.S Puttaswamy v. Union of India

(52) The Supreme Court in *K. S. Puttaswamy v. UoI* held that - "the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III (fundamental rights) of the Constitution."

(53) Sydney Li, Jamie Williams, Despite What Zuckerberg's Testimony May Imply, AI Cannot Save Us, EFF (Nov 10, 2018, 11:05AM), https://www.eff.org/deeplinks/2018/04/despite-what-zuckerbergs-testimony-may-imply-ai-cannot-save-us/

(54) Natasha Duarte, Emma Llanso, Anna Loup, Mixed Messages? The Limits of Automated Social Media Content Analysis Presented at the 2018 Conference on Fairness, Accountability, and Transparency, Natasha Duarte Emma Llansó (Center for Democracy & Technology), Anna Loup (University of Southern California), (Jan 10, 2019, 12:00PM), https://cdt.org/files/2017/12/FAT-conference-draft-2018.pdf

(3) Accurate text classification requires clear, consistent definitions of the type of speech to be identified. Policy debates around content moderation and social media mining tend to lack such precise definitions;

(4) The accuracy and intercoder reliability challenges documented in NLP studies warn against widespread application of the tools for consequential decision-making; and

(5) Text filters remain easy to evade and fall far short of humans' ability to parse meaning from text.

(C) Local Office, Incorporation and Appointment of Nodal Officer: Rule 3(7) of the Draft Rules requires all intermediaries with more than 5 million users in India to be incorporated, have a permanent registered office in India with a physical address and appoint a nodal officer and a senior functionary for 24-hour coordination with Law Enforcement Agencies. At present there is lack of clarity about what this number of users refers to i.e. whether it refers to daily, monthly or yearly users, or the number of total registered users. To understand the implication of this requirement, reference to the user base of popular messaging apps is pertinent. WhatsApp, India's most popular chatting app, has around 200 million users in India. Relatively newer chatting applications Hike[55] and ShareChat[56] have 100 million users and 25 million users respectively. The 5 million users specified in the Draft Rules represent around 1% of the Internet user base in India which might bring a substantial number of intermediaries under a new set of compliance requirements. This may cause many start-ups to bear the brunt of high costs stemming from incorporation under the Indian companies law - the Companies Act, 2013.

(D) Ambiguous Terms: The Draft Rules contain mandates regarding a broad category of content that is classified as 'unlawful'. Such a broad category of content described using terms such as "grossly harmful", "harassing" and "blasphemous" could result in a chilling effect with intermediaries being forced to remove even lawful content.[57]

Intermediary Liability in Reality

Shreya Singhal brought in a welcome respite to Internet intermediaries in India as they no longer were required to act upon sundry requests for content takedowns and could rely on court orders or notifications of authorised government agencies. This judgment also upheld constitutionally guaranteed rights of free speech of citizens on the Internet and clarified that restriction on speech will need to be within the contours of Article 19(2) of the Constitution, the court held that -

"86. That the content of the right under Article 19(1)(a) (free speech right) remains the same whatever the means of communication including Internet communication is clearly established …"
Problems remain though, constitutional limits on free speech like - the security of the state, public order, decency/ morality, defamation or incitement to an offence are not defined, there are various tests established by courts for each of these limits but they are to be determined based on the facts and circumstances of each case. The ambiguity surrounding the meaning of these words and phrases might make it difficult for intermediaries to act upon orders received from competent authorities based on these limits.

Phrases used in the Intermediaries Guidelines, which online platforms are required to incorporate in their terms and conditions remain vague and undefined. According to these, content that is grossly harmful, hateful and blasphemous must not find a place on intermediary platforms. Following *Shreya Singhal*, such mandate must come from courts or the government, but plat-

---

(55) Jon Russell, Hike unbundles its messaging app to reach India's next wave of smartphone users, TECHCRUNCH (Dec 4, 2018, 10:08AM) https://techcrunch.com/2018/01/16/hike-unbundles-its-messaging-app/.
(56) Aria Thaker, Indian politicians are now flocking to an unlikely "no English" social network, QUARTZ (Nov.11, 2018, 3:00PM) https://qz.com/india/1414241/sorry-facebook-indias-bjp-and-congress-flock-to-sharechat/
(57) Such chilling effect has already been witnessed as a result of Section 66A

forms might takedown similar content relying on their community guidelines or terms and conditions, which may lead to private censorship.

Then there is the reality of online platforms being utilised by bad actors to disseminate disinformation, terrorist content, child pornography etc. pushing governments around the world to hold intermediaries more accountable for third party content on their platforms. In India, public lynchings which have been attributed to rumour mongering on intermediary platforms have resulted in the government wanting to bring in changes such as - automated content filtering and traceability, which will have negative effects on rights like free speech and privacy. Countries across the world are pressuring intermediaries to be more responsible for the content flowing through their platforms. Though intermediary liability needs to be revisited in the current global context, any changes to law and regulation must ensure that it doesn't abrogate basic human rights.

Content takedown requests are sometimes also received by intermediaries in the form of orders of law enforcement agencies under Section 91 of the Code of Criminal Procedure,1973 ("CrPC"). [58] Section 91 empowers courts and authorised police officers to 'summon' produce 'any document or other thing' which may be required for conducting investigation.[59] The IT Act, gives enough powers to central and state governments for intercepting, monitoring, decrypting and taking down content from their platforms. [60] No part of Section 91 of the CrPC gives powers to law enforcement agencies to have content taken-off online platforms, it only provides for summoning of documents for aiding investigation. Despite the specific applicability of the IT Act in matters of online content,[61] law enforcement agencies fall back on general laws such as the CrPC to issue orders for content takedowns. The courts in India have held intermediaries more accountable for IP protected content flowing through their channels, which has been discussed in the next section.

3.5 Intermediary Liability and IP Disputes in India

The intermediary liability law in India is primarily governed by Section 79 of the IT Act as discussed above. As per that provision, online intermediaries enjoy a safe-harbour for third-party content on their platforms, till they prescribe to certain due diligence rules set out under the Intermediaries Guidelines. Provisions under the Copyright Act, 1957 provide for some protection to certain intermediaries as well[62]. Section 79 of the IT Act in conjunction with the ruling of the Supreme Court of India in Shreya Singhal, which broadened the protection given to intermediaries and allowed them to takedown content only on instructions by courts or authorised government agencies, is the authoritative law of the land on intermediary liability. Though, it is important to point out that in terms of intellectual property rights ("IP rights"), courts in India have placed a higher responsibility on intermediaries to take down content content that infringes IP rights.

Liability under the IT Act

Beyond Section 79 of the IT Act, Section 81 is a non-obstante clause, providing for an overriding effect of the IT Act over all other laws in times of conflict. But, this clause carves out an exception for copyright and patent holders.[63]

The Intermediaries Guidelines also require intermediaries to notify their users for not uploading content that - *"infringes any patent, trademark, copyright or other proprietary rights"*[64] and to not

---

(58) S.91 of CrPC - the Omnipotent provision? by SFLC.in, can be accessed here - https://sflc.in/s91-crpc-omnipotent-provision

(59) Certain intermediaries stated that Section 91 of the CrPC is being used for taking down content.

(60) Section 69 and 69A of the IT Act, available in the annexure

(61) As discussed previously, Section 81 of the IT Act precludes the applicability of other laws in terms of conflicting provisions.

(62) Section 52(b) and (c) of the Copyright Act, 1957 in the annexure.

(63) Section 81 of the IT Act: Act to have overriding effect. – The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force.
[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).]

(64) Rule 3(2)(d) and Rule 3(3) of the Intermediaries Guidelines in the annexure

host/ publish such content on their platforms.

Limited and Conditional Protection under the Copyright Act, 1957 ("the Copyright Act")

Section 52(b) and (c) of the Copyright Act provides protection to intermediaries for transient or incidental storage of copyrighted works, if:

(a) It is purely in the technical process of electronic transmission or communication of such content;

(b) It is for the purpose of providing links or access/ integration to content, when not expressly barred by the copyright owner and when the intermediary does not have reasonable grounds for believing that such storage is of an infringing copy (actual knowledge requirement).

Section 52(c) also provides for a notice and takedown mechanism, wherein copyright owners could request intermediaries to remove protected content from their platforms for a minimum period of 21 days (or for a longer period in case of a court order mandating such requirement). As per this provision, intermediaries on being satisfied are required to remove content within 36 hours of being intimated.[65]

Thus, reading the IT Act and the Copyright Act in conjunction, in cases of content protected by copyright, intermediaries must prescribe to a higher standard of care in ensuring that their platforms are not used to make infringing content available to the general public. It is also worthwhile to note that the Copyright Act does not define what is 'transient or incidental storage' and without such clarity, ambiguity remains on which intermediaries are protected/ unprotected under this clause.

3.5.1 The IP Effect - Distinguishing Actual Knowledge from Shreya Singhal

As discussed at the starting of this section, according to Section 79, safe-harbour protection is available to intermediaries in India if they, upon receiving 'actual knowledge', remove unlawful content from their platforms. This 'actual knowledge' was interpreted to mean intimation by appropriate government agency or an order of a court by the Supreme Court in *Shreya Singhal*, but subsequently in matters concerning the infringement of IP rights, courts have distinguished the 'actual knowledge' requirement as enunciated in *Shreya Singhal* and replaced it with a 'specific knowledge' requirement i.e. if intermediaries are given specific knowledge of infringing works by IP owners, they are liable to take it down to keep their safe-harbour protection under the IT Act.

In its landmark judgment in *Myspace v. Super Cassettes Industries*[66] the Delhi High Court while distinguishing copyright matters from those contained under Article 19(2) of the Constitution of India[67] stated that -
"50. … In the case of copyright laws it is sufficient that MySpace receives specific knowledge of the infringing works in the format provided for in its website from the content owner without the necessity of a court order."

Reiterating the actual knowledge requirement in cases of content protected by copyright, the court stated that -
"57. … If copyright owners, such as SCIL inform MySpace specifically about infringing works and despite such notice it does not takedown the content, then alone is safe harbor denied. However, it is for SCIL to show that despite giving specific information the appellant did not comply with its notice."

Apart from distinguishing the actual knowledge requirement in cases of copyright, the Myspace judgment is also important since it clarified that unspecified material, including takedowns of all future infringing content is not what intermediaries are required to do under law as this will lead to private censorship and will have a chilling effect on free speech.

---

(65) Section 52(c) of the Copyright Act and Rule 75 of the Copyright Rules, 2013 in the annexure
(66) Myspace v. Super Cassettes Industries Ltd., 236 (2017) DLT 478
(67) In *Shreya Singhal*, the Supreme Court restricted takedown requests to matters contained under Article 19(2) of the Constitution of India

The court held that -

"62. … The remedy here is not to target intermediaries but to ensure that infringing material is removed in an orderly and reasonable manner. A further balancing act is required which is that of freedom of speech and privatized censorship. If an intermediary is tasked with the responsibility of identifying infringing content from non-infringing one, it could have a chilling effect on free speech; an unspecified or incomplete list may do that. … Such kind of unwarranted private censorship would go beyond the ethos of established free speech regimes."

In another matter before the Delhi High Court,[68] this time for the infringement of a design under the Designs Act, 2000, the rights owner wanted the intermediary (eBay) not only to remove existing infringing products but to screen similar listings in future and remove infringing products without the intimation of the owner. The court rejecting such a claim held that intermediaries cannot be expected to exercise such vigilance over their platforms and are liable to only remove infringing content which is specifically asked for. The court held that -

*"**35**. … Moreover the question, whether an IP right has been infringed or not is more often than not a technical question with which the courts steeped in law also struggle and nothing in the IT Act and the IT Rules requires an intermediary, after having been once notified of the IP Rights, not allow anyone else to host on its portal infringing goods/matter. The intermediaries are not possessed of the prowess in this respect. As aforesaid, it is a different matter, when attention of the intermediary is invited to infringing product and complaint made with respect thereto. Merely because intermediary has been obliged under the IT Rules to remove the infringing content on receipt of complaint cannot be read as vesting in the intermediary suo motu powers to detect and refuse hosting of infringing contents."*

More recently, the same court in *Christian Louboutin v. Nakul Bajaj,*[69] a matter relating to trademark infringement held an e-commerce company not be an intermediary as per Section 79 of the IT Act [70] and held that for e-commerce portals to claim exemption under the safe-harbour provision, they need to ensure a passive and not an active participation in the selling process. The court held that -

"78. … When an e-commerce company claims exemption under Section 79 of the IT Act, it ought to ensure that it does not have an active participation in the selling process. The presence of any elements which shows active participation could deprive intermediaries of the exemption."

With respect to IP rights, taking into consideration the law and the above mentioned judicial pronouncements, the following inferences can be made:

(a) Despite the ruling of the Supreme Court of India in Shreya Singhal, courts have distinguished the 'actual knowledge' requirement for matters of free speech[71] from claims of IP infringement. In cases of IP, courts have operationalised the notice and takedown mechanism, wherein rights owners can request for infringing content to be taken off by intermediaries on intimating them of the infringement (the notice and takedown mechanism); and

(b) Such requests need to be specific and not broad, rights owners may not request intermediaries to be vigilant about all future violations, as this will require constant monitoring/ screening, which is outside the role played by intermediaries (the specific knowledge requirement);

None of the cases discussed above, eventually lead to revocation of intermediary safe-harbour to either place primary or contributory liability for infringement on the Internet platforms. In Christian Louboutin, though the Delhi High Court held that due to the active role played by

---

(68) Kent RO Systems Ltd. v. Amit Kotak, [240 (2017) DLT3]
(69) Christian Louboutin SAS v. Nakul Bajaj, [253(2018)DLT728]
(70) Though the definition of intermediary as per the IT Act specifically includes - online auctions sites and online marketplaces. Kindly refer to Section 2(1)(w) of the IT Act.
(71) As guaranteed by the Indian Constitution under Article 19(1)(a)

the e-commerce portal in selling activities it did not fall into the definition of an intermediary, the court didn't hold the portal liable for trademark infringement.

Due to the lack of clarity on intermediary liability, for content protected by IP rights, uploaded to platforms by third parties, intermediaries will end up over complying with takedown requests to ring fence their safe harbour protection. This may have a negative effect on content which falls under 'fair use/ fair dealing' categories of law, [72] severely impacting the free-speech rights of citizens. This, coupled with the fact that tech giants like - Facebook, Google and Twitter already use automated filters which often lead to taking down legal content, could prove to be problematic for the digital rights of Indian people.

Though courts have recognized that intermediaries cannot and should not play the role of judges in determining what is illegal or legal content,[73] by empowering rights owners to send notices for specific content removal, courts have also made it difficult for intermediaries to defend instances of fair use/ fair dealing.

In a recent draft policy document issued by the Department for Promotion of Industry and Internal Trade,[74] the government has raised issues around the liability of e-commerce platforms for counterfeit and pirated products. The draft policy has recommended that if trade mark owners require, e-commerce platforms shall not list their products without prior consent. On the copyright front, the draft policy has recommended that, *"Intermediaries shall put in place measures to prevent online dissemination of pirated content."* The draft policy reiterates the 'specific knowledge' requirement and the 'notice and takedown' mechanism established by courts (as discussed above) - *"Upon being notified by the owner of copyright protected content/ work that a website or e-commerce platform is making available, selling or distributing the copyrighted content/ work without the prior permission/ authorization of the owner, such website or platform should expeditiously remove or disable access to the alleged content."*

The draft e-commerce policy has used both terms - e-commerce platforms and intermediaries, creating further confusion. The way e-commerce platforms function in India, any demands for ensuring non-listing of products may lead to pre-screening which will dilute the safe-harbour protection granted to such platforms under law. Pre-screening and active monitoring of content has also been held to be not required by law and may have a chilling effect on free speech (as observed in the *Myspace* judgment). In terms of copyright violation, though the draft policy is in line with the current jurisprudence, this does create disproportionate pressure on intermediaries to takedown content, which may not be illegal and also makes intermediaries the judges of what is legal/ illegal.

The growing trend of making intermediaries more liable for the content on their platforms is apparent from the draft policy's demand on such services to show a higher level of 'social responsibility'. The draft policy states that intermediaries need to ensure 'authenticity' and 'genuineness' of content flowing through their pipelines - "*… With a growing importance of these entities, their social responsibilities also increases. Due to the fact that traders, merchants, individual users, organizations, associations are all dependent on them, the authenticity of content posted on their websites cannot be compromised. In this regard, it is important to emphasize on responsibility and liability of these platforms and social media to ensure genuineness of any information posted on their websites.*"

From a policy standpoint this is problematic for various reasons, firstly, this recommendation uses very broad and vague phrases like social responsibility, authenticity and genuineness; secondly, this makes intermediaries

---

(72) Divij Joshi, SaReGaMa Pa-rdon Me, You Have the Wrong Address: On the Perils and Pitfalls of Notice and Takedown, SPICY IP (Feb 13, 2019, 11:05PM) https://spicyip.com/2019/02/saregama-pa-rdon-me-you-have-the-wrong-address-on-the-perils-and-pitfalls-of-notice-and-takedown.html

(73) Supra 68

(74) Draft National e-Commerce Policy, India's Data for India's Development, Department of Industrial Policy and Promotion (Feb 25, 2019, 4:15PM) https://dipp.gov.in/whats-new/draft-national-e-commerce-policy-stakeholder-comments

the judges of deciding what is legitimate and what is not, which will have the unintended consequence of private censorship (this is also held to be illegal by various courts); thirdly, it is very difficult to ascertain the authenticity and genuineness of content, whether protected by IP rights or not, as it may depend on various factors which a machine or even a human reviewer may find it hard to determine. As iterated at various points in this report, any suggestions/ recommendations for increasing the accountability of intermediaries must not abrogate free speech and privacy rights of netizens.

3.6 Indian courts on intermediary liability

Having gone over the applicable laws with regard to intermediary liability in India, this section of the report will examine some of the notable cases around intermediary liability in India. Only cases from various High Courts (at the state level) and the Supreme Court of India have been considered for this section, and the list is non-exhaustive. The cases discussed herein are relevant to provide an overview of the jurisprudence which has evolved in India on issues surrounding intermediary liability

3.6.1 Avnish Bajaj v. State[75] (2008)

As discussed previously, this case was an inflection point for the debate on intermediary liability in India. For a detailed discussion on Avnish Bajaj and what the court held in it, please refer to the section 3.1.

This case holds importance in the intermediary liability landscape in India as for the first time the managing director of a company (in this situation eBay) was charged with criminal provisions both, under the penal law of India and under the IT Act, for content circulated by a third party on an e-commerce platform. In this matter, Avnish Bajaj escaped liability on technical grounds as the company Baazee.com was not arraigned as an accused in both matters - before the High Court and subsequently the Supreme Court of India. Another important aspect of this case (the Delhi High Court judgment) was that the court recognized the use of content filters for blocking pornographic content and stated that companies bear the risk of acquiring knowledge if such content escapes the filters.[76]

3.6.2 Google v. Visakha Industries[77] (2009)

In 2009, Visakha Industries, a construction company involved in the manufacturing of asbestos cement sheets, filed a criminal defamation case against Ban Asbestos Network India (BANI), its coordinator and Google India. It alleged that the coordinator of BANI had written blog posts on a website owned by BANI, that contained scathing criticism of the company and therefore harmed its reputation in the market. Google India was also arraigned as a party in the litigation because the blogpost was hosted on the blog publishing service of Google.

Google India moved the High Court of Andhra Pradesh for dismissal of the criminal charges against it on the grounds that it enjoyed safe-harbour protection under Section 79 of the IT Act. It was contended that Google is not the publisher or endorser of the information, and only provides a platform for dissemination of information. It, therefore cannot be held liable. The High Court refused to accept Google's contention and dismissed the petition on the grounds that Google failed to take appropriate action to remove the defamatory material, in spite of receiving a take-down notice from the company.

Aggrieved by the judgment of the High court, Google filed an appeal in the Supreme Court in 2011, where the matter is currently pending.

3.6.3 Shreya Singhal v. Union of India[78] (2015)

As discussed previously, the Shreya Singhal judgment was a watershed moment for the the debate on intermediary liability in India (for a detailed discussion of the Shreya Singhal judgment, kindly refer to the section - The Intermediary Liability Regime in India.)

---

(75) Supra 30

(76) Post this judgment, the intermediary law of India was amended, as discussed in the section 3.1.

(77) Google v. Visakha Industries, [Criminal Petition No. 7207 of 2009]

(78) Supra 41

3.6.4 Myspace Inc. vs. Super Cassettes Industries Ltd.[79] (2017)

This case is important from a copyright perspective as the division bench of the Delhi High Court in this matter reversed a single judge decision holding Myspace liable for copyright infringement. The division bench held that if intermediaries are tasked with the responsibility of identifying illegal content, it could have a chilling effect on free speech. For a detailed discussion on what the court held in Myspace, kindly refer to the section 3.1.

In this matter, the court also distinguished the 'actual knowledge' requirement from Shreya Singhal to mean 'specific knowledge' in matters of copyright infringement i.e. if intermediaries are pointed to specific infringing material by rights holders then they must remove such content, without the necessity of a court order.

3.6.5 Kent RO Ltd & Anr. Vs. Amit Kotak & Ors[80] (2017)

In January, 2017, a single judge bench of the Delhi High Court, refused to compel intermediaries to screen content that infringes intellectual property laws on an ex-ante basis.[81]

The petitioner Kent RO Systems, a company that manufactures water purifiers filed for permanent injunction against one Amit Kotak (respondent) for infringing its intellectual property rights by copying its designs and eBay India Pvt Ltd. for aiding the infringement by allowing the respondent to sell its product on their website.

eBay India Private Limited sought the protection of Section 79 of the IT Act, under which it is saved from any liability arising out of third party generated information, data or communication link established by it, as long as its function is confined to providing access to a communication system.

The single judge bench of Justice Rajiv Sahai Endlaw held that compelling an intermediary to screen content would be *"an unreasonable interference with the rights of the intermediary to carry on its business."*[82]

The court also asserted that requiring an intermediary to screen any kind of content would change the role of an intermediary from a facilitator to an adjudicator. Under Section 79 and the IT Rules, 2011, an intermediary is only obliged to remove content on receipt of a court order or Government notification.

In Kent RO, the court reiterated the specific knowledge requirement as expounded in Myspace, stating that when the attention of the intermediary is brought to infringing products, then they are liable to remove such listings from their websites.

3.6.6 The Registrar (Judicial), Madurai bench of Madras High Court v. The Secretary to Government, Union Ministry of Communications, Government of India, New Delhi and Ors.[83] (2018)

This case arose from the unfortunate circumstance of the death of a 19-year old student, allegedly after playing the online game "The Blue Whale Challenge". This game required players to undertake 50 extreme tasks which eventually lead to them committing suicide. The Madras High Court took suo motu cognizance of the matter as there was public interest at play.

The court had asked the government to request online services like Google, Facebook, Microsoft, Yahoo and Instagram to remove 'links' of the blue whale game from their portals. To this, Google replied by stating that its Indian subsidiary cannot remove content as their app store was run by the parent company, which was governed by US laws. Google clarified, that their team in the

---

(79) Myspace Inc. vs. Super Cassettes Industries Ltd. [236 (2017) DLT 478]
(80) 2017 (69) PTC 551 (Del)
(81) R. Bajaj, In a Welcome Development, Delhi High Court Refuses to Compel Intermediaries to Screen Content Violative of Intellectual Property Laws on an Ex-ante Basis, SpicyIP (June 20, 2018, 8:30PM) https://spicyip.com/2017/03/in-a-welcome-development-delhi-high-court-refuses-to-compel-intermediaries-to-screen-content-violative-of-intellectual-property-laws-on-an-ex-ante-basis.html , last accessed 20 June 2017.
(82) 2017 (69) PTC 551 (Del)
(83) 2018 (1) CTC 506

US was aware of the game and will continue to take action against providers who violate their app store policies.

The court, while highlighting Google's response and noting how difficult it is for law enforcement to get access to crucial information, reprimanded online services stating that they cannot abdicate their duties and responsibilities under law -

"The service providers cannot abdicate their responsibilities. They cannot also plead that they have no control over the content. A mere look at the net neutrality debate that is presently going on would show that the service providers are in a position to have control over the content that passes through their information highway. If the service providers can attempt to control the content for commercial considerations, they can certainly be called upon to exercise their power of control in public interest also. Rather they must be mandated to do so."

The court thus directed the Central Government to take appropriate steps to bring "Over The Top" services into a legal framework obliging them to comply with the laws of India and to provide the required information to the law enforcing agencies - "Methods must to be devised to ensure that those OTTs which could not be brought within such framework are not accessible in India." The court also requested the government to amend laws and regulations so that Indian laws are applicable to these foreign services and law enforcement can get access to relevant information at crucial points.

This case highlights an important pain point in the current intermediary liability debate, not just in India, but around the world i.e. access to information by law enforcement. The government, while introducing changes like the Draft Rules (in reference to the previous section), often point to this problem highlighting the fact that foreign entities take refuge behind source country laws at the time of providing assistance to Indian law enforcement agencies. It will remain to be seen how tech-companies and governments solve the problem of access to information by law enforcement, but any new changes will have to be in consonance with free speech and privacy rights.[84]

3.6.7 Christian Louboutin SAS v. Nakul Bajaj and Ors[85] (2018)

In November 2018, the Delhi High Court laid down certain guiding principles in respect of liability of e-commerce platforms for trademark infringement.

The plaintiff, Christian Louboutin, a company that manufactures high end luxury shoes, was the owner of registered trademarks in India and sold its products only through authorized dealerships. The defendant, Darveys.com was an e-commerce platform that markets itself as a "luxury brands marketplace." The plaintiff alleged that the defendant sells counterfeit products bearing the plaintiff's name on its website. Apart from offering for sale and selling the Plaintiff's products, on the website of the defendant, it also alleged that the defendant used the names "Christian" and "Louboutin" as meta tags to attract traffic towards its website, and this resulted in infringement of the trademark rights of the Plaintiff, and violation of personality rights of Mr. Christian Louboutin, the founder of the brand.

The defendant argued that the goods sold were genuine, and that there was no infringement on its part because it was a mere intermediary, and entitled to protection under Section 79 of the IT Act.
The High Court examined in detail what constitutes an 'intermediary' under Section 2(w) of the IT Act, and whether online marketplaces as intermediaries qualify for safe harbour protection under Section 79.

In determining the role of an online marketplace and ambit of 'service' as has been used in the definition of 'intermediaries' under the IT Act, the court laid down twenty six tasks that an intermediary may undertake, ranging from iden-

(84) The IT Act gives the government powers to request for information, intercept, decrypt and also takedown content as per Section 69 and 69A (kindly refer to Chapter IV of this report).
(85) Christian Louboutin SAS v. Nakul Bajaj & Ors, Civil Suit No. 344/2018

tification of the seller, advertising products on the platform, transporting the product to the purchaser, using trademarks through meta tags, among other things.

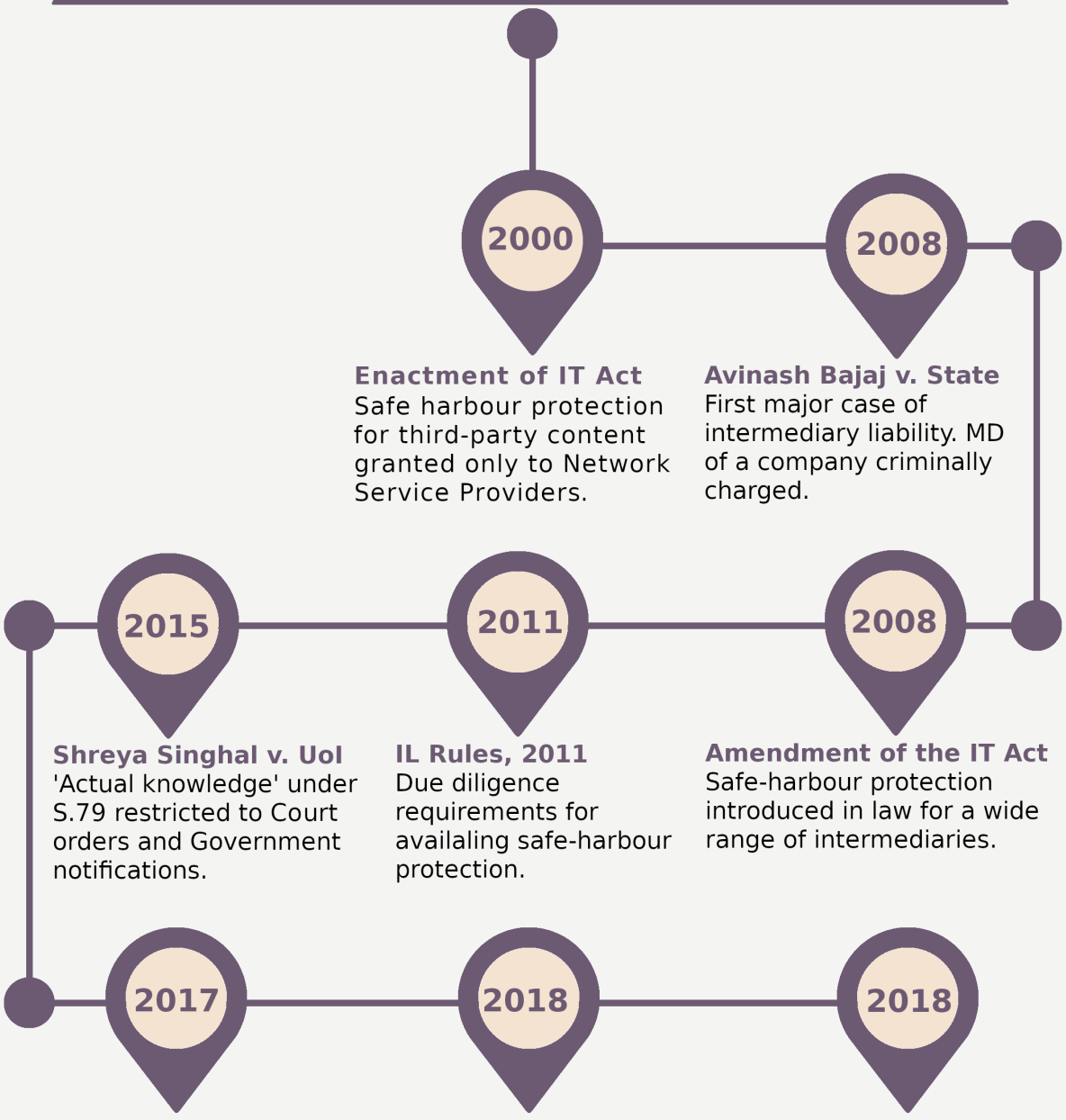
The judgment also stated that it has to be seen whether the platform is taking adequate measures to ensure that no unlawful acts are committed by the sellers. Measures include the manner in which the terms of the agreements entered into between the sellers and the platform are enforced, consequences of violation of the terms, among others.

The Court noted that the elements summarised above would be key to determining whether an online marketplace or an e-commerce website is 'conspiring, abetting, aiding or inducing' and is thereby contributing to the sale of counterfeit products on its platform. *"When an e-commerce website is involved in or conducts its business in such a manner, which would see the presence of a large number of elements enumerated above, it could be said to cross the line from being an intermediary to an active participant",* the judgment stated.

After considering all the above mentioned factors, the Court concluded that Darveys.com cannot be termed as an intermediary that is entitled to protection under Section 79 of the IT Act.

This case is particularly important because it was the first time that the Court decided on the issue of trademark infringement by online e-commerce platforms that have maintained that they are immune from liability by virtue of Section 79 of the IT Act. It is also pertinent to mention that the court despite ruling that Darveys.com was not an an intermediary, it did not hold it liable for trademark infringement.

A BRIEF TIMELINE OF INTERMEDIARY LIABILITY LAW IN INDIA



Intermediary Liability 2.0: A Shifting Paradigm

sflc.in

CHAPTER IV

EXPANDING OBLIGATIONS OF INTERMEDIARIES

Although Section 79 of the IT Act provides safe-harbour protection to intermediaries from liability arising out of third-party content, with the intermediaries' primary obligation in this regard being that unlawful content be taken down on receipt of a court order or Government directive, a number of petitions have been filed before various Indian courts seeking to expand the scope of intermediaries' obligations with respect to user-generated content. These petitions filed before various High Courts and the Supreme Court have been observed to attempt and partially succeed at broadening the scope of obligations in two major directions i.e. proactive monitoring of content, and Right to be Forgotten.

4.1 Proactive Monitoring of Content

Despite the Supreme Court's judgment in *Shreya Singhal*, in which the Court clarified that intermediaries are not responsible for judging the legitimacy of content on their platforms, the last two years have seen litigation that involved intermediaries to act as content monitors. A few notable cases are:

4.1.1 Sabu Mathew George v. Union of India[86]

In 2008, Sabu Mathew George, a gender activist and doctor, filed a writ petition in the Supreme Court of India to ban advertisements related to pre-natal sex determination from search engines like Google, Bing and Yahoo. It was contended by the petitioner that the display of these results violated Section 22 of the Pre-Conception and Pre-Natal Diagnostic Techniques (Prohibition of Sex Selection) Act, 1994 ("PCPNDT Act"). In their reply, the respondents argued that they are "conduits" and not content providers and hence protected under Section 79 of the IT Act. It was also argued that there are innumerable activities banned by law, but their information is still available online and offline. Disentitling anyone from receiving information or gaining knowledge on a subject is violative of Article 19(1)(a) of the Constitution, which includes the right to know and right to receive or access information.

Over the course of proceedings, the court issued interim orders directing Google, Microsoft and Yahoo to 'auto-block' pre-natal sex determination ads from appearing in search results. The court also drew a list of forty key

(86) AIR 2018 SC 578

words that were to be auto-blocked if anyone attempts to look them up. Expert in-house committees were directed to be formed by search engines to evaluate and delete content violative of Section 22 of the PCPNDT Act "based on its own understanding."

The Supreme Court also directed the Central Government to constitute a nodal agency for receiving complaints from anyone who came across anything that has the nature of an advertisement or has any impact in identifying a boy or a girl in any method, manner or mode by any search engine. The nodal agency was then required to convey actionable complaints to the concerned intermediaries, who were obliged to delete the content in question within 36 hours and intimate the nodal agency.

This petition was disposed off in December 2017, with the apex court issuing additional directions to the newly formed nodal agency and expert committee to hold a meeting with the assistance of the petitioner's legal team, "so that there can be a holistic understanding and approach to the problem". Google, Yahoo and Microsoft were also directed to work with the committee to identify and implement a "constructive and collective approach to arrive at a solution".

Significance: In this matter, the Supreme Court of India stated that intermediaries are obliged to keep unlawful content from appearing on their networks. Even after the ruling of the Supreme Court in Shreya Singhal, wherein the court made it clear that intermediaries must not be asked to exercise their personal judgment in determining the legality of content for takedown purposes, the court continues to ask intermediaries to proactively filter their platforms for illegal content. Such decisions by courts contribute to the confusion over the level of due diligence which is to be followed by intermediaries to protect their safe-harbour.

4.1.2 Kamlesh Vaswani v. Union of India[87]
This public interest litigation was filed by an Indore based lawyer before the Supreme Court of India challenging Sections 66, 67, 69, 71, 72, 75, 79, 80 and 85 of the IT Act as being unconstitutional, as they were argued to be inefficient in tackling the rampant availability of pornographic material in India. These provisions were said to be ineffective as the IT Act was primarily meant to govern e-commerce and e-governance and was therefore not suited to tackle cyber crimes including the distribution of pornographic content online.

The petitioner prayed, among other things, to declare the above mentioned provisions unconstitutional, draft a national policy and draft an action plan to tackle pornography, and to declare the watching of pornographic videos as a non-bailable, cognizable offense. During arguments in court the petitioner also prayed that intermediaries be asked to proactively filter out pornographic content from public access. Though, the court appeared somewhat sympathetic to the petitioner's grievances, concerns about technical feasibility and privacy implications of proactive filtration of content were expressed by the presiding judges. The Cyber Regulations Advisory Committee, which was directed by the Court to explore ways to block pornographic content online, tasked the Internet and Mobile Association of India with identifying a list of websites to be blocked. Interestingly, 857 pornography websites were blocked by the Indian Government in August 2015, but these were all unblocked within a few days. This matter is currently pending before the Court.

Significance: This matter once again seeks to impose proactive content monitoring obligations on online intermediaries, this time by blocking access to pornographic content. It is pertinent to note that the presiding judges had recognized the technical challenges involved in filtering the Internet of all pornography and also touched upon the fact that what an individual does in the privacy of his/her home is not for the state to dictate. However, the Court has also expressed that it is necessary to keep more harmful forms of pornography like child porn at bay and that intermediaries may be under an obligation to proactively block access to such content.

---

(87) [W.P.(C) No. 177/2013]

4.1.3 In Re: Prajwala[88]

Sunitha Krishnan, founder of Hyderabad-based NGO Prajwala, wrote a letter to the Supreme Court of India highlighting the issue of videos of sexual violence floating on WhatsApp and other social media platforms. She submitted a list of the websites that were airing the videos and requested, among other things, that the Ministry of Home Affairs be directed to look into the matter with the help of intermediaries like Google, YouTube and Facebook. The Supreme Court's social justice bench took suo moto cognizance of the letter and ordered a Central Bureau of Investigation (CBI) inquiry into the videos. The Department of Telecommunications (DoT) and the Ministry of Home Affairs were also directed to put the concerned web portals under the scanner.[89] Furthermore, a Committee was constituted under the Chairmanship of Dr. Ajay Kumar, the then Additional Secretary of the Ministry of Electronics and IT, to assist and advice the court on the feasibility of preventing sexual abuse/violence videos from appearing online.

Over the course of the proceedings, the Committee held extensive deliberations involving a number of representatives from various intermediary platforms, lawyers, academics and civil society members. A two-part report was also submitted by the Committee based on its deliberations, containing some recommendations towards preventing the upload and circulation of sexually abusive/violent videos online. All parties including Google, Facebook, Microsoft, Yahoo!, WhatsApp and the Government were directed by the Court to implement all recommendations with consensus at the earliest. The matter is still pending before the Court awaiting final disposal.

Significance: This matter raises important questions with regard to the role of intermediaries in controlling the propagation of videos depicting sexual abuse and violence. This also ties in to challenges with regard to formulation of policies to tackle the issue of circulation of non consensual sexually explicit videos, such as revenge porn on the Internet. Interestingly, many of the accepted recommendations of the Ajay Kumar Committee involved blocking of search queries containing certain key words and preventing upload of sexually abusive/violent videos at the source using hashing and other technologies. While the recommendations are currently being considered as voluntary initiatives to be undertaken collaboratively by stakeholders, it could be problematic if they come to be treated as legal mandates with mandatory compliance. It is pertinent to note that the SC imposed costs of Rs. 100,000 each on Google, Facebook, Microsoft, Yahoo! and WhatsApp for failing to file replies describing steps taken by them to give effect to the Committee's recommendations.

4.2 Right to Be Forgotten

The Right to be Forgotten is a civil right recognized in many jurisdictions that allows individuals to demand erasure of their personal information from the Internet. It gives individuals the right to control their personal information on the Internet. The roots of this right arises from the right to privacy and right to reputation. The concept was developed in the EU and Argentina and has been in practice since 2006. Google's Transparency Report on search removals under European privacy law shows a steady increase in "requests to delist" and "URLs requested to be delisted" from May 2014.[90] By January 2019 the number increased to 777,706 requests to delist and 3,006,188 URLs requested to be delisted.[91]

For the purpose of better understanding, this right may be divided into: 'Right of Erasure' and 'Right to Delist'. The right of erasure is when the data is deleted from the source and

---

(88) SMW (Crl) No. 3/2015

(89) B. Sinha, SC orders CBI probe into rape videos circulated on WhatsApp, HINDUSTAN TIMES (June 25, 2018, 5:23PM) http://www.hindustantimes.com/india/sc-orders-cbi-probe-into-rape-videos-circulated-on-whatsapp/story-6OUlIUVqd0n-VqKHrXPxyeK.html

(90) Search Removals under Privacy Law, Google Transparency Report, GOOGLE (Feb 26, 2019, 12:00PM) https://transparencyreport.google.com/eu-privacy/overview?hl=en

(91) Id.

therefore completely deleted from the Internet. Whereas the right to delist pertains to the search results no longer being linked to the name or identity of the data subject with the data still existing on the web. It is debatable which of these rights must be preferred over the other. The earliest example of usage of this right is that of a criminal's right to not be linked with their crime for the entirety of their life so that he may be rehabilitated into society again.

The legitimacy of this right is fiercely contested on the grounds that it negatively affects freedom of speech and expression and the right to access information. On the other hand, advocates of this right argue that digital technology allows storage of large amounts of data on the Internet which preserves an unnatural memory. Individuals should have right over their personal information. In other words, the right to be forgotten is an essential safeguard to right to informational self determination and the right to privacy.

The right to be forgotten has evolved differently in different jurisdictions. Germany and France had recognized the right long before the Google Spain ruling which brought the RTBF challenge to prominence[92]. The US does not have a specific legislation with respect to privacy. While there seems to be a greater inclination toward freedom of speech and expression, there have been many cases which have upheld the right to be forgotten and have ordered that data be delisted. These include protection of minors, deletion of criminal records and individual bankruptcy.[93] Argentina currently grapples with the balance between freedom of speech and expression and the right to privacy, where many individuals have filed cases for the delisting of links which contain their personal data. Though, the case of Virginia da Cunha, where the complaint was regarding the linking of the complainant's name with pornographic websites ended in defeat, it brought Argentina into the spotlight with respect to the debate on the right to be forgotten.[94]

In India, the right to be forgotten has not been formally recognized yet (India's Draft Personal Data Protection Bill, 2018 provides for a right to be forgotten - which is a right to restrict/ prevent the disclosure of information and not a right of erasure)[95] but has been evolving through decisions rendered by various courts. The doctrine came up before consideration for the first time in April 2016 before the High Court of Delhi.

There have been instances when the courts have asked for particular judgments or personal information to be removed from online repositories or search engine results.
A few noteworthy cases that highlight the evolution of this concept in India are mentioned below:

4.2.1 Laksh Vir Singh Yadav v. Union of India & Ors.[96] (2016)
In this case, the petitioner had made a request to Indian Kanoon and Google to expunge his name from their search results as it was affecting his employment opportunities.
He contended that the criminal case between his wife and mother kept showing in the results, every time his name was searched on the Internet, which gave the impression that he was involved in the matter.

The matter is ongoing in the High Court of Delhi and the next hearing is scheduled for July 18, 2019.

4.2.2 [Unknown] X v. Union of India [97] (2016)
The petitioner had moved the High Court of Kerala against Google, seeking removal of hateful content from the Internet posted by his former wife. He alleged that a Google search

---

(92) Ioania Stupariu, Defining the Right to be Forgotten: A comparative Analysis between the EU and US, CENTRAL EUROPEAN UNIVERSITY, 2015
(93) Id.
(94) Id.
(95) Kindly refer to Section 27 of the Draft Personal Data Protection Bill, 2018, which can be accessed, here - https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018_0.pdf
(96) W.P. (C) 1021/2016
(97) W.P (C) No. 8477/2016

would end up in certain web links defaming him and his children, causing them immense humiliation.[98] The petitioner cited the Google Spain decision, wherein the Court of Justice of the EU had ruled that Google must create a system by which it can be asked to remove personal data, on the request of an individual. Though this matter has been disposed off as per the Kerala High Court's website, the final order of the court is not available. On the petitioner's name, the case status mentions - *'X - Name and Address of the Petitioners Deleted'*.[99]

4.2.3 Sri Vasunathan v. The Registrar[100] (2017)
The petitioner had filed a writ petition in the High Court of Karnataka, seeking removal of his daughter's name from an earlier order passed by the court with respect to a criminal case involving her and the defendant. According to the petitioner, a name search on search engines like Google and Yahoo revealed that she was embroiled in the dispute, thus harming her marital relationship and reputation in society.

The court granted the request and made the following observation: "This would be in line with the trend in western countries of the 'right to be forgotten' in sensitive cases involving women in general and highly sensitive cases involving rape or affecting the modesty and reputation of the person concerned."
The Court also directed its registry to ascertain that the petitioner's daughter's name is not reflected on the Internet, with regard to the criminal matter, thus upholding her right to be forgotten.

4.2.4 Dharmraj Bhanushankar Dave v. State of Gujarat[101] (2015)
The petitioner in this case was acquitted in a previous criminal matter in the Gujarat High Court and the judgment was supposed to be non-reportable. However, indiankanoon.org published the judgment on their web portal and it was available via a simple Google search. Aggrieved by the same, the petitioner approached the High Court of Gujarat seeking deletion of the judgment from the website as it was affecting his personal and professional life.

Rejecting the petitioner's plea and dismissing the petition, the court held that the High Court is a court of record and Rule 151 of the Gujarat High Court Rules, 1993 provides that copies of documents in any civil or criminal proceeding and copies of judgment of the High Court can be given, even to third parties with the order of the Assistant Registrar. According to the High Court, the petitioner had not been able to point to any provision of law by which the Respondent could be restrained under Art 226 of the Constitution. The court refused to accept the argument put forth by the petitioner that publication of the judgment was violating his Right to Life and Personal Liberty under Article 21. The Court further stated that publishing on the website would not amount to being reported, as the word " reportable" only refers to it being reported in the law reporter.
Thus, it can be seen that even though currently there isn't a statutory right to be forgotten in India, courts have requested search engines to delist content from their platforms. It is important to point out that successful RTBF requests in India have only lead to delisting of posts from search engines and not deletion of content from the source.

4.3 Intermediary perspectives
As part of the research, a number of intermediaries were approached to solicit their views on India's intermediary liability framework and the expanding content obligations brought about by the recently proposed Draft Rules and judicial pronouncements. Said intermediaries included leading social media platforms, search engines, and consumer review websites, as well as start-ups and small businesses

---

(98) Marital discord has Google in dock, THE DECCAN CHRONICLE (June 6, 2018, 5:05PM), http://www.deccanchronicle.com/nation/current-affairs/040316/marital-discord-has-google-in-dock.html
(99) For the case status , kindly refer to - https://services.ecourts.gov.in/ecourtindiaHC/cases/case_no.php?state_cd=4&dist_cd=1&court_code=1&stateNm=Kerala#
(100) 2017 SCC Kar 424
(101) 2015 SCC Guj 2019

offering specialized services online.

Every intermediary that was spoken with held the view that the current legislative framework is adequate in principle. The IT Act explicitly provides safe harbour protection under Section 79, exempting intermediaries from liability for user generated content, so long as they exercise no editorial control. The Intermediaries Guidelines Rules then lay down a set of due diligence conditions that must be met before qualifying for immunity under Section 79. While the language of the Intermediaries Guidelines created some confusion initially and resulted in intermediaries having to exercise their personal judgment when responding to takedown requests and over-complying to err on the side of caution, the Supreme Court's decision in Shreya Singhal was said to be of tremendous help in clarifying the state of law. By virtue of the judgment, intermediaries are no longer required to takedown content upon receiving requests from third-parties, which led to a very significant drop in the number of such requests received.

On the Draft Rules, the intermediaries were of the view that the rules should not be applied uniformly to all categories of service providers, there should be a function based approach and regulation should tie to the different functions that intermediaries play on the Internet. It was felt that Rule 3(2) of the Draft Rules should be less vague and more specific and should not contain large, all-encompassing terms, such as - grossly harmful, harassing, blasphemous etc. This would entail intermediaries to act as adjudicators to takedown content and lead to private censorship.

It was opined that the traceability requirement under Rule 3(5) of the Draft Rules is not framed clearly and the terms "enable tracing" lacks clarity. Also, enforcing this requirement would impact the trust that customers place on any sort of digital transaction.

Intermediaries pointed out that mandatory incorporation under the Companies Act, 2013, along with appointing a nodal officer will increase the cost and compliance burden of smaller intermediaries. It was also mentioned that the 24-hour requirement to remove content will be difficult to comply with due to technological challenges. Such a requirement doesn't leave scope for review of takedown orders. Automated tools for takedowns further aggravate these problems and takes away the review process. This also affects fair use and fair dealing activities under copyright law. A review mechanism should be in place, which gives scope to intermediaries for checking the veracity of takedown orders. Intermediaries recommended that, a graded approach to takedown could be implemented. More sensitive content like – terrorist content or child pornography could be treated more expeditiously as compared to other requests.

On the usage of automated tools to proactively monitor content, it was felt that asking intermediaries to proactively filter their networks of impermissible content under threat of legal consequences overlooks certain ground realities. This was also said to be contrary to the prevailing jurisprudence of various courts in the country.

Firstly, an intermediary's function is limited to providing a platform for its users to publish content or avail services. The intermediary by definition does not play a role in deciding what content is published or what services are offered/availed on its platform. Safe harbour protection is provided to intermediaries on the basis of this very premise – that it would be unjust to hold platform providers answerable under law for content/services that they have no connection with.

Secondly it is in the intermediary's own business interest to keep their platforms free from unlawful or otherwise harmful content, as users will naturally tend to avoid using inhospitable platforms. However, considering the sheer volume of activity that takes place on intermediary platforms on a daily basis, exhaustive filtering of impermissible content is impossible even after dedicating vast resources to do this. A large intermediary said that it has set up

dedicated facilities and devoted vast numbers of personnel all over the world to review content that potentially violates its terms of use. It has also begun to implement automated review and takedown processes with the help of algorithms and artificial intelligence in limited contexts. Despite such measures, comprehensive filtration of impermissible content remains elusive due to the millions of data points that are generated on a daily basis. Assigning legal penalties for failure to proactively remove impermissible content would be crippling for its business, leading to a situation where it would be forced to adopt overbroad measures that will inevitably affect legitimate content as well as free speech rights. Significant variance amongst national laws with regard to permissibility of certain types of content was also identified as a critical bottleneck for intermediaries with a global presence. It was felt that emphasis when it comes to content regulation should be on self-regulatory or co-regulatory models, where the intermediaries are allowed the bandwidth to develop and use their own internal processes to identify and remove impermissible content while operating under the ambit of safe-harbour protection from legal liability over user-generated content.

Though intermediaries agreed that in principle Shreya Singhal provided a much needed clarification in law, they also said that significant problems remained with the implementation of the Shreya Singhal judgment, especially in the lower judiciary. Several intermediaries were of the view that judges of lower courts are woefully unaware of intermediary liability laws. For instance, many judges remain ignorant of the Supreme Court's verdict in Shreya Singhal, exempting intermediaries from acting on takedown requests sent by third-parties, prompting them to issue verdicts unfavourable to intermediaries. Though, such verdicts are usually set aside on appeal, they nevertheless tie up intermediaries for weeks, months and years in needless litigation incurring great costs. Awareness building amongst judges on intermediary liability laws as well as broader technology laws was therefore highlighted as a priority.

On the issue of 'Right to be Forgotten', the intermediaries reported that they had received RTBF requests and such requests were mostly for reputational harm.

In conversation with intermediaries, some of them stated that sometimes, they receive orders from law enforcement agencies to takedown content from their platforms under Section 91 of the CrPC. This provision, empowers law enforcement agencies to request for 'any document or other thing' which would assist them in conducting investigation. Though, there are relevant provisions under the IT Act for production and removal of content (Section 69 and 69A of the IT Act), law enforcement agencies continue to use provisions under other laws which may lack the procedural safeguards installed under the provisions of the IT Act and its rules therein.

The table below shows the different stances that various intermediaries and industry associations have taken on changes introduced in the Draft Rules. Due to their far reaching effects on the intermediary landscape in India, this analysis is restricted to issues such as - i) traceability of originator of information; ii) local incorporation requirement; and iii) deployment of automated tools for content filtering.[102]

The organizations that support a particular provision of the Draft Rules, their respective position has been marked by ✔ . The organizations that oppose a particular provision in the Guidelines, their stance is depicted by ✕.

Several intermediaries, both domestic and foreign, were approached, but not all of them provided their response

(102) This information has been compiled based on the public submissions of the entities mentioned herein, to the government consultation held on the Draft Rules.

Analysis of submissions sent to the Ministry of IT by various intermediaries/ industry associations

S.No.	Organization (Associations and Corporations)	Traceability [Rule 3(5)]	Incorporation under Companies Act, 2013 [Rule 3(7)]	Deployment of automated tools for pro-active content monitoring [Rule 3(9)]
01	Wipro	----	✔	✔ [Provided that there are certain measures to reinstate genuine content]
02	Freedom Publishers Union	✘	----	----
03	Asia Internet Coalition	✘	✘	✘
04	ITU-APT Foundation of India	✘ [For lack of clarity of the purpose of seeking certain data and the obligations of intermediaries for the same]	✘	✘
05	The Indian Music Industry	----	----	✔
06	The Information Technology Industry Council	✘	✘	✘
07	Computer and Communications Industry Association-US	✘	✘	✘

08	Broadband India Forum	✗	✗	✗
09	CCAOI	✗	✗	✗
10	ISPAI	✔ [Provided that the terms "lawful order" and "Government Agency" are defined. Also, it should be clarified that the Rule applies only to platform based services.)	✔	✔ [Provided that the Rule is only applicable to platform based services]
11	Asia Cloud Computing Association	✗	✗	✗
12	IAMAI	✗	✗	✗
13	CII	✗	✗	✗
14	BSA	----	----	✗
15	NASSCOM	✗	✗	✗
16	Mozilla	✗	✗	✗
17	India Tech	✔	✔	✔
18	COAI	✗	✔	✗
19	Xiaomi	✔ [Provided that the power to enable tracing should be derived out of sections 69, 69A or 69B of the IT Act. Moreover, the intermediary shall on a best efforts basis enable tracing. In case it is not able to do so, it shall provide reasons in writing.]	✔ [Only specific intermediaries, as notified by the Government, should be required to incorporate under the Companies Act, 2013]	✗

20	Amcham India	✗	----	✗
21	Jio	✔	✔	✔
22	Star India	----	----	✔
23	ShareChat	✗	✔	✗
24	Bombay Chamber of Commerce and Industry	✔ [Provided that requests under this Rule should be made only if it is required for investigation, detection, prosecution or prevention of an offence. Further, language should be modified to refer to information within the intermediary's position. Furthermore, 'government agency' should be defined and limited.]	✔ [Only applicable to specifically notified intermediaries.]	✗
25	IBM	✔ [Provided there are enough safeguards]	----	✗
26	FICCI	✗	✗	----
27	ASSOCHAM	✗	✗	✗
28	Large multinational software company (did not want to be quoted)	✗	✗	✗
29	Large multinational technology company (did not want to be quoted)	✗	✗	✗
30	MouthShut.com	✗	✗	✗

On an analysis of the table, it can be stated that only a handful of organizations (6 out of 31) agreed to some form of a traceability requirement. Barring Xiaomi and IBM (both of which asked for more safeguards) all other organizations which agreed to the traceability requirement were Indian in origin.

A quarter of all organizations (8 out of 31) were agreeable to the incorporation requirement, all of which were Indian organizations except for Xiaomi.

On automated content filtering, again, only 6 out of 31 organizations were in acceptance of the requirement - all of these were Indian companies/ associations.

Internet Service Providers Association of India, IndiaTech, Reliance Jio and Bombay Chamber of Commerce and Industry - agreed to all 3 proposed changes (traceability, incorporation and automated content filtering).

Star India and the Indian Music Industry, that specifically deal with copyrighted content, have supported the requirement for automated content takedowns. The reasons for espousing it, as given in their comments is to protect the intellectual property rights of artists and content creators and to curb online piracy.

From this data it can be gathered that Indian businesses are leaning more towards stricter government regulation on online intermediaries. Such regulation will grant Indian businesses greater control over what flows through their pipelines, and at the same time weaken free speech and privacy rights online.

CHAPTER V

THE MANILA PRINCIPLES – A COMPARATIVE ANALYSIS

The Manila Principles is a set of guidelines outlining safeguards that must apply in all legal frameworks on intermediary liability. The document was launched at RightsCon, Southeast Asia – a multi-stakeholder conference held in Manila, Philippines in 2015 – by a coalition of Internet rights activists and civil society organizations. The main purpose of the Manila Principles is to encourage the development of interoperable and harmonized liability regimes that can promote innovation while respecting users' rights in line with the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and the United Nations Guiding Principles on Business and Human Rights.[103]

The six broad principles are as follows.[104]
(1) Intermediaries should be shielded by law from liability for third-party content.

(2) Content must not be required to be restricted without an order by a judicial authority.

(3) Requests for restrictions of content must be clear, be unambiguous, and follow due process.

(4) Laws and content restriction orders and practices must comply with the tests of necessity and proportionality.

(5) Laws and content restriction policies and practices must respect due process.

(6) Transparency and accountability must be built in to laws and content restriction policies and practices.

By virtue of offering safe-harbour protection to Internet intermediaries under Section 79 of the IT Act, India can be said to comply with the first of these principles (Intermediaries should be shielded by law from liability for third-party content). The immunity enjoyed by intermediaries is of course conditional, and there is ambiguity in law that make compliance far from easy, yet immunity under law is nevertheless provided for.

(103) Manila Principles on Intermediary Liability, MANILA PRINCIPLES (Feb 16, 2019, 7:09PM), https://www.manilaprinciples.org/
(104) Id

The second of the Manila principles (content must not be required to be restricted without an order by a judicial authority) is more or less respected under Indian intermediary liability laws, as intermediaries are required to take-down content only on receiving a court order or Government directive asking them to do so. Though government directives are not orders by judicial authorities, it must be noted that Indian laws do not ask intermediaries to exercise their own judgment in taking down content. Intermediaries are no longer obligated to remove content on receiving notices from any affected third-party. Rather, an independent determination as to whether or not particular content should be removed is taken by the judiciary or executive, then conveyed to intermediaries (for takedowns in situations of IP disputes, there still exists a notice-and-takedown regime, at the behest of the rightsholder).[105]

The third Manila principle (requests for restrictions of content must be clear, be unambiguous, and follow due process) does not see much compliance in the Indian legal framework. It can be argued that takedown orders issued by the judiciary or executive or those received under the Copyright Act are bound to be clear, unambiguous and in compliance with due process, in that the orders will always clearly direct takedowns, specify the particular content to be removed and be authorized by relevant law. However, intermediaries also receive what are effectively takedown orders through other channels, such as Section 91 of the CrPC, which does not have the requisite checks and balances in place against abuse.

The fourth principle (laws and content restriction orders and practices must comply with the tests of necessity and proportionality) is not fully observed in India, most notably in cases of alleged copyright infringement. Indian courts routinely issue website blocking orders to intermediaries like ISPs on the basis of petitions alleging copyright infringement against a large number of websites at once. It is not uncommon for such orders to target thousands of websites and URLs at the same time, a large number of which may not even contain infringing material. As the lists of websites and URLs to be blocked are so populous, it can be said with certainty that no detailed examinations of alleged infringements are undertaken before issuing takedown orders, and even in cases where copyright infringement does exist, whole websites are frequently directed to be taken down even if specific URLs within these websites will suffice.

The fifth Manila principle (laws and content restriction policies and practices must respect due process) is not fully observed in India. With respect to legal provisions specifically related to intermediary liability i.e. Section 79 of the IT Act and the Intermediaries Guidelines Rules, deviations from due process include the absence of opportunities for content creators to defend their content, and the absence of means to restore content that has already been removed. As for provisions that are unofficially used to direct content takedowns like Section 91 of the CrPC, the question of due process does not even arise because such provisions are not rightfully to be used for this purpose.

The final Manila principle (transparency and accountability must be built in to laws and content restriction policies and practices) too does not find compliance in India, especially with regard to content taken down under Section 69A of the IT Act. Rules framed under Section 69A stipulate that strict confidentiality must be maintained around complaints made, orders issued and action taken under the provision, and reasons for takedowns are never disclosed to the public. Websites and URLs blocked under Section 69A simply state that blocking order have been received from the Government. Moreover, requests made under the Right to Information Act for details on blocked content are consistently turned down by citing the confidentiality clause built into the regulation.

In review, India's compliance with the Manila principles, though improved over the past few years, is still wanting in many respects.

---

(105) Kindly refer to the 'IP Effect - Distinguishing Actual Knowledge from Shreya Singhal' section of the report.

CHAPTER VI

INTERMEDIARY LIABILITY IN OTHER JURISDICTIONS

Different jurisdictions may establish different enactments and procedures to restrict content that is considered unlawful. Different regimes also follow different legal frameworks to grant conditional immunity or safe harbour to intermediaries. The notice and notice model obliges intermediaries to direct any complaint of alleged infringement of copyright they get from the owner of copyright to the user or subscriber in question. This procedure is followed in Canada and is enshrined in the Copyright Modernization Act, that came into effect in January, 2015. According to this model, receiving a notice does not compulsorily mean that the subscriber has infringed copyright and does not require the subscriber to contact the copyright owner or the intermediary.[106] Therefore, the objective of the notice-and-notice regime is to discourage online infringement on the part of Internet subscribers and to raise awareness in instances where Internet subscribers' accounts are being used for such purposes by others.[107] It enables the complainant and the content owner to resolve the dispute among themselves without the involvement of the intermediary.

The second model is the notice and takedown model. It is followed by countries like South Korea[108] and the United States of America.[109] According to this system, an intermediary responds to government notifications, court orders or notices issued by private parties themselves, to take down content by promptly removing or disabling such allegedly illegal content. This self regulatory framework, by which ISPs determine whether or not a website contains illegal or harmful content raises questions of accountability, transparency and the overall appropriateness of delegating content regulation to private actors, who have to act as judges.[110] This could be seen as "privatization of censorship."[111]

---

(106) The US Copyright Modernization Act 2015
(107) Office of Consumer Affairs (OCA), Notice and Notice Regime, Innovation Science and Economic Development Canada (Mar 9, 2019, 1:48 PM), https://ic.gc.ca/eic/site/oca-bc.nsf/eng/ca02920.html
(108) The South Korea Copyright Act 1957 § 103
(109) Digital Millennium Copyright Act 1998 § 512(c)
(110) Christian Ahlert, Chris Mrasden and Chester Yung, How Liberty Disappeared from Cyber space: The Mystery Shopper Tests Internet Content Self Regulation, THE PROGRAMME IN COMPARATIVE MEDIA LAW AND POLICY, UNIVERSITY OF OXFORD (9 Mar, 2019, 2:00 PM), http://pcmlp.socleg.ox.ac.uk/wp-content/uploads/2014/12/liberty.pdf
(111) Id.

The third model is called the Graduated Response model or the "three strikes system." Under this system, rights holders may ask intermediaries to send warnings to subscribers identified as engaging in illegal file sharing or infringing copyright. The intermediary may be required to send more than one notice, with repeat infringers risking bandwidth reduction and sometimes even complete suspension of the account. France, New Zealand, Taiwan, South Korea and the United Kingdom have enacted legislations that require intermediaries to exercise certain degree of policing to protect users' rights. Some countries like the United States and Ireland permit private arrangements between rights holders and intermediaries to accomplish the same end.

6.1 United States of America

The law relating to intermediary liability in the United States of America is mostly governed by Section 512(c) of the Digital Millennium Copyright Act ("DMCA") and Section 230 of the Communications Decency Act ("CDA").
Section 512 of the DMCA was enacted by the US Congress with a view to limit the liability of intermediaries and to check online and copyright infringement, including limitations on liability for compliant service providers to help foster the growth of Internet-based services.[112] The intermediary must comply with the notice-and-takedown procedure under Section 512 to qualify for protection.

The CDA was originally enacted to restrict freedom of speech and expression but the restrictive sections were later struck down for being unconstitutional. Section 230 is considered one of the most valuable tools for protecting intermediaries from liability for third party generated content. It reads: *"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."* The section encompasses claims of defamation, encroachment of privacy, tortious interference, civil liability for criminal law violations, and general negligence claims based on third party content.[113]

The legislation also contains a policy statement from the US government that provides safe harbour at Section 230(B)(4) for any action taken to: *"encourage the development of technologies that maximize user control over what information is received by individuals to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material."*

In 2018, a new legislation called Stop Enabling Sex Traffickers Act was passed (SESTA) and Allow States and Victims to Fight Sex Trafficking Online Act (jointly known as FOSTA-SESTA), which expands criminal liability for classifieds websites like Backpage.com which was alleged to host ads from sex traffickers in its adult services action. Backpage.com had claimed that it is an intermediary and is not responsible for content uploaded by users. Although, the new bill is well-intentioned, it dilutes the protection provided by Section 230 of the Communications Decency Act, which has been considered the most valuable piece of legislation protecting freedom of speech and expression online, by implicating intermediaries for user generated content.

6.1.1 Case Studies

6.1.1.1 Dart v. Craigslist, Inc.[114]

Craigslist is the largest online classified advertisement service in the United States. Postings on the site include advertisements for jobs, housing, sale of various items and other services. The listings also included a section

---

(112) The US Copyright Modernization Act 2015
U.S. Copyright Office, Section 512 Study, COPYRIGHT.GOV (9 Mar, 2019, 2:04 PM), https://www.copyright.gov/policy/section512/
(113) Adam Holland, Chris Bavitz, Jeff Hermes, Andy Sellars, Ryan Budish, Michael Lambert and Nick Decoster Berkman Center for Internet & Society at Harvard University, Intermediary Liability in the United States, PUBLIXPHERE (9 Mar, 2019, 2:04 PM), https://publixphere.net/i/noc/page/OI_Case_Study_Intermediary_Liability_in_the_United_States
(114) [665 F. Supp. 2D 961]

for "erotic services", even though Craigslist's terms and conditions categorically forbid the advertisement of illegal activities.

The "erotic services" section caught the attention of State and local law enforcement. It was seen that some users were using the section to advertise illegal services. In March 2008, the Attorney General of Connecticut, on behalf of the Attorney Generals of forty other states sent a notice to Craigslist to remove the ads that publicized prostitution and other illicit activities prohibited under state law. In November 2008, Craigslist reached an agreement with the Attorney Generals to implement steps to hinder illegal listings on the erotic services section, but not completely remove them. Subsequently, Craigslist announced a ninety percent drop in its erotic services listings.

Four months later, Craigslist was sued by one Thomas Dart, a Sheriff for the county in Illinois, claiming that the site created "public nuisance", under Illinois state law, because its *"conduct in creating erotic services, developing twenty-one categories, and providing a word search function causes a significant interference with the public's health, safety, peace, and welfare."*[115] Craigslist ultimately won that case on the grounds of Section 230(c)(1) of the CDA. The court held that Craigslist was an Internet service provider (Intermediary) and hence, immune from wrongs committed by third parties. However, Craigslist removed the phrase "erotic services" and replaced it with "adult services." The case is considered a victory for online speech.

Later, due to mounting pressure, Craigslist completely removed the "adult services" section from its website and the link to the section was replaced with a black label reading "censored."

6.1.1.2 Viacom International, Inc v. YouTube, Inc. [116]

In March 2007, Viacom filed a lawsuit against Google and YouTube alleging copyright infringements by its users.

It sought USD 1 Billion in damages for the copyright infringement of more than a hundred thousand videos owned by Viacom. Thereafter, several class action lawsuits were also filed against YouTube by sports leagues, music publishers and other copyright owners.

These lawsuits tested the strength of the DMCA safe harbour as applied to online service providers that host text audio and video on behalf of users.[117] In June 2010, the United States District Court for the Southern District of New York held that YouTube, being an intermediary was protected by the DMCA safe harbour. The judge said that compelling online platforms to constantly police videos that are being uploaded by third parties *"would contravene the structure and operation of the DMCA."* [118] Viacom appealed the decision to the Second Circuit Court of Appeals in August 2011, which reversed the earlier decision. In April 2013, the district again ruled in favour of YouTube saying that YouTube could not possibly have known about the copyright infringements and was protected under the DMCA. Viacom again began the process of second appeal but before the date of the hearing, both the parties negotiated a settlement in March 2014.[119]

6.1.1.3 Matthew Herrick v. Grindr LLC [120]

Plaintiff Herrick alleged that his ex-boyfriend set up several fake profiles on Grindr (a dating

---

(115) Thomas Dart, Sheriff of Cook County V. Craigslist, Inc, 665 F. Supp. 2d 961

(116) [No. 07 Civ. 2103 2010 WL 2532404 (S.D.N.Y 2010)]

(117) Viacom v. YouTube, Electronic Frontier Foundation (Feb 20, 2019, 12:00PM) https://www.eff.org/cases/viacom-v-youtube

(118) Miguel Helft, Judge Sides With Google in Viacom Suit Over Videos, NEW YORK TIMES (Feb 20, 2019, 12:05PM), http://www.nytimes.com/2010/06/24/technology/24google.html?_r=0

(119) Jonathan Stempel, Google, Viacom settle landmark YouTube lawsuit, REUTERS (Feb 20, 2019, 3:09PM), http://www.reuters.com/article/us-google-viacom-lawsuit-idUSBREA2H11220140318

(120) 17-CV-932 (VEC)

app for the LGBTQ community) that claimed to be him and resulted in identity theft/ manipulation. Over a thousand users responded to the impersonating profiles. Herrick's ex boyfriend, pretending to be Herrick, would then direct the men to Herrick's' workplace and home.

The impersonating profiles were reported to Grindr (the app's operator), but Herrick claimed that Grindr did not respond, other than to send an automated message. Herrick sued Grindr, accusing the company of negligence, intentional infliction of emotional distress, false advertising, and deceptive business practices for allowing him to be impersonated and turned into an unwitting beacon for stalkers and harassers[121] liable to him because of the defective design of the app and the failure to police such conduct on the app.

The Court rejected Herrick's claim that Grindr is not an interactive computer service as defined in the CDA. With respect to Grindr's products liability, negligent design and failure to warn claims, the court found that they were all predicated upon content provided by another user of the app. Any assistance, including algorithmic filtering, aggregation and display functions that Grindr provided to his ex boyfriend was "neutral assistance" that is available to good and bad actors on the app alike.

The court also highlighted that choosing to remove content or to let it stay on an app is an editorial choice, and finding Grindr liable based on its choice to let the impersonating profiles remain would be finding Grindr liable as if it were the publisher of that content.

An appeal has been filed against the court's ruling to the Second Circuit Court of Appeals, in this matter.

6.2 European Union

6.2.1 E-commerce Directive

Articles 12 to 15 of Directive 2000/31/EC of 8 June 2000 on electronic commerce mandate the member states of the EU to establish defenses, under both civil and criminal law for the benefit of certain types of online intermediary.[122] Directive 2001/29/EC on Copyright in the Information Society (as to copyright) and Directive 2004/48/EC on the Enforcement of Intellectual Property Rights (other than copyright) mandate EU member states to give rights holders the right to seek an injunction against those online intermediaries whose services are used by a third party to infringe an intellectual property right.

Articles 12 to 15 of Directive 2000/31/EC is the primary piece of legislation governing intermediary liability. It incorporates a notice-and-takedown system for intermediaries to abide to. Articles 12 to 14 categorises intermediaries into "mere conduits" , 'caching' services and 'hosting' services. Article 15 states that intermediaries have no general obligation to actively monitor the information which they transmit or store for illegal activity.

The General Data Protection Regulation ("GDPR") which came into effect from 25th May 2018[123] is aligned with Directive 2000/31/EC. Article 2(4) of the GDPR reads:

"This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive."

Recital 21 of the GDPR[124] reads as follows: *"This Regulation is without prejudice to the*

---

(121) Andy Greenberg, Spoofed Grindr Accounts Turned One Man's Life Into a 'Living Hell' , WIRED (Feb 20, 2019. 5:40PM), https://www.wired.com/2017/01/grinder-lawsuit-spoofed-accounts/

(122) Trevor Cook, Online Intermediary Liability in the European Union, 17, JOURNAL OF INTELLECTUAL PROPERTY RIGHTS, 157-159 (2012)

(123) The History of the General Data Protection Regulation, EUROPEAN DATA PROTECTION SUPERVISOR (Jan 20, 2019, 2:30PM) https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

(124) A copy of the GDPR can be downloaded from here - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

application of Directive 2000/31/EC of the European Parliament and of the Council, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive. That Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between Member States."

6.2.2 Directive on Copyright in the Digital Single Market COM/2016/0593 final - 2016/0280 (COD) (EU Copyright Directive)

In September of 2016 the EU Commission proposed a new directive to update its existing copyright framework[125] after a number of years of public consultation. Since then several negotiations and amendments have been incorporated in the proposal and a final text [126] was agreed upon by the EU Parliament and Council on 13th of February, 2019.[127]

Two provisions, in particular, in the proposed EU copyright directive, warrant red flags: Article 11 and Article 13.

Article 11, grants publishers the right to request payment from online platforms that share their stories. This provision is being called the "link tax" which gives publishers the right to ask for paid licenses when online platforms and aggregators such as Google news share their stories.[128] The Article excludes 'uses of individual words or very short extracts of a press publication' from its purview.[129]

The more problematic provision of the proposed directive is, however, Article 13, which makes 'online content sharing service providers'[130] liable for copyright infringement for content uploaded by their users. The proposed copyright directive precludes the 'safe-harbour' protection afforded to such online content sharing service providers, under the EU e-commerce directive, for user generated content which is protected by copyright,. For protection against liability, these services must enter into license agreements; make best efforts to get such authorisation for hosting copyright protected content and make best efforts to ensure unavailability of protected content (this will likely result in the use of upload filters) [131]; and implement a notice and takedown mechanism, including prevention of future uploads.

This effectively means that intermediaries will have to proactively monitor and prescreen all the content that users upload. This degree of monitoring for illegal content is not possible manually and can only be handled by automated filters, that are far from perfect and can be easily manipulated. For

---

(125) Hayleigh Bosher, Keeping up with the Copyright Directive, IPKITTEN (9 Mar, 2019, 2:14 PM), https://ipkitten.blogspot.com/2019/02/keeping-up-with-copyright-directive.html

(126) Proposal For A Directive Of The European Parliament And Of The Council On Copyright In The Digital Single Market, JULIA REDA (9 Mar, 2019, 2:20 PM), https://juliareda.eu/wp-content/uploads/2019/02/Copyright_Final_compromise.pdf

(127) Id.

(128) Matt Reynolds, What Is Article 13? The EU's Divisive New Copyright Plan Explained, WIRED (9 Mar, 2019, 2:23 PM), https://www.wired.co.uk/article/what-is-article-13-article-11-european-directive-on-copyright-explained-meme-ban

(129) Christiane Stuetzle and Patricia C. Ernst, European Union: The EU Copyright Directive Hits The Homestretch, MONDAQ (9 Mar, 2019, 2:26 PM), http://www.mondaq.com/unitedstates/x/786366/Copyright/The+EU+Copyright+Directive+Hits+The+Homestretch

(130) This includes - online intermediaries who store and give access to a large amount of copyright protected content or other protected content uploaded by its users. This specifically excludes - non profit online encyclopedias, non profit educational and scientific repositories, open source software developing and sharing platforms, online marketplaces and B2B cloud services and cloud services for users. Kindly refer to Article 2(5) of the proposed copyright directive.

(131) Christiane Stuetzle and Patricia C. Ernst, European Union: The EU Copyright Directive Hits The Homestretch, MONDAQ (9 Mar, 2019, 2:26 PM), http://www.mondaq.com/unitedstates/x/786366/Copyright/The+EU+Copyright+Directive+Hits+The+Homestretch

example, YouTube's "Content ID" system has been deemed notorious for over-removing innocent material.[132] Article 13 will turn intermediaries into the content police and would hamper the free flow of information on the Internet.[133] There is also the problem of dedicated infringers finding a way around content filters and the possibility of automated tools making errors, specially in cases of fair use like - criticism, reviews and parodies.[134]

The proposed directive is scheduled for voting before the European Parliament either in late March or mid-April of 2019.

6.2.3 Terrorist Content Regulation[136]

On 12th September 2018, the European Commission released the draft - 'Regulation on Preventing the Dissemination of Terrorist Content Online.' which requires tech companies and online intermediaries to remove "terrorist content" within one hour after it has been flagged to the platforms by law enforcement authorities as well as Europol. [137] The proposal needs to be backed by member states and the EU Parliament before it can be passed as law.

Websites that fail to take immediate action will be liable to pay fines. Systematic failure to comply will invite penalties of up to four percent of the company's global turnover in the last financial year (similar to fines under the GDPR)[138]. Requirement for proactive measures, including automated detection, are needed to effectively and swiftly detect, identify and expeditiously remove or disable terrorist content and stop it from reappearing once it has been removed. A human review step before content is removed, so as to avoid unintended or erroneous removal of content which is not illegal has also been recommended in the proposed regulation.[139]

These draft legislations in the EU, namely - the proposed copyright directive and the terrorist content regulation, point towards a shifting trend in European countries wherein governments wanting to hold online intermediaries more accountable and responsible for illegal user generated content generated on their platforms.

In both cases, for copyright and terrorist content, the EU has suggested (through these legislations) the use of automated tools for content filtering, which may lead to over-compliance (to ring-fence themselves against liability), private censorship and resultant dilution of free speech rights on the Internet.

6.3 Case studies

6.3.1 Delfi v. Estonia[140] (2015)

The judgment in this case brings to light fascinating issues of both human rights and the law governing intermediary liability in the EU, making it one of the most important judgment of recent times, with respect to intermediary liability.

Delfi is one of the biggest online news portals in Estonia. Readers may comment on the news stories, even though Delfi operates a system

---

(132) Cory Doctorow, Artists Against Article 13: When Big Tech and Big Content Make a Meal of Creators, It Doesn't Matter Who Gets the Bigger Piece, ELECTRONIC FRONTIER FOUNDATION (9 Mar, 2019, 2:26 PM), https://www.eff.org/deeplinks/2019/02/artists-against-article-13-when-big-tech-and-big-content-make-meal-creators-it

(133) Id.

(134) Id.

(135) Cory Doctorow, The Final Version of the EU's Copyright Directive Is the Worst One Yet, ELECTRONIC FRONTIER FOUNDATION (9 Mar, 2019, 2:26 PM), https://www.eff.org/deeplinks/2019/02/final-version-eus-copyright-directive-worst-one-yet

(136) European Commission, Proposal For A Regulation Of The European Parliament And Of The Council On Preventing The Dissemination Of Terrorist Content Online, EUROPEAN COMMISSION (9 Mar, 2019, 2:35 PM), https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-preventing-terrorist-content-online-regulation-640_en.pdf

(137) Id. Articles 4, 13

(138) Id. Article 18

(139) Id. Article 6

(140) Delfi v. Estonia, 64569/09, ECtHR (2015)

to regulate unlawful content within a notice and takedown framework. In January, 2006, a news article was published by Delfi that talked about how a ferry company, namely SLK Ferry had wrecked the pathway that connected Estonia's mainland to its islands. There were one hundred and eighty five user generated comments on the news article, out of which about twenty were viewed as offensive and threatening towards the company's sole shareholder L. The comments were asked to be removed and damages were claimed by L. Delfi removed the comments but refused to pay damages. The matter was brought to various lower courts before it reached the Supreme Court in June 2009, which held that Delfi had a legal obligation to prevent unlawful and illegal content from being posted on their website, since it was the publisher of the comments, along with the original author, and therefore was not protected by EU Directive 2000/31/EC. Further, the court stated that defamatory speech is not covered under right to freedom of expression.

Aggrieved by the Supreme Court's judgment, Delfi moved the European Court of Human Rights. The question before the ECHR was whether the previous court's decision to hold Delfi liable was an unreasonable and disproportionate restraint on Delfi's freedom of expression, according to Article 10[141] of the Convention for the Protection of Human Rights and Fundamental Freedoms.

The ECHR was called upon to strike a balance between freedom of expression under Article 10 of the Convention and the preservation of personality rights of third persons under Article 8 of the same Convention.[142] In 2013, in a unanimous judgment, Delfi lost the case at ECHR and the matter was thereafter brought before the Grand Chamber. On 16 June, 2015, the Grand Chamber upheld the decision of the Fifth Section of the ECHR, asserting that the liability against Delfi was justified and proportionate because:

(1) The comments in question were outrageous and defamatory, and had been posted in response to an article that was published by Delfi on its professionally managed online news portal which is of commercial nature; and
(2) Delfi failed to take enough steps to remove the offensive remarks immediately and the fine of 320 Euros was insufficient.[143]

The decision was criticized by digital and civil rights activists for being against Directive 2000/31/EC which protects intermediaries from user generated content and freedom of expression online. It also set a worrying precedent that could change the dynamics of free speech on the Internet and intermediary liability. Furthermore, the decision was condemned for the Court's fundamental lack of understanding of the role of intermediaries.

6.3.2 Magyar Tartalomszolgáltatók Egyesülete ("MTE") and Index.hu Zrt ("Index") v. Hungary[144] (2016)

After the controversial Delfi judgment, which was considered by many a setback to online free speech and liability of intermediaries with respect to third party generated content, the European Court of Human Rights delivered another landmark judgment, ruling the other way.

The parties, MTE and Index are a Hungarian self regulatory body of Internet content providers and a news website respectively. The organizations had featured an opinion piece on the unethical business practices of a real estate company, which garnered a lot of resent-

---

(141) Council of Europe, European Convention on Human Rights, EUROPEAN COURT OF HUMAN RIGHTS (Feb 9, 2019, 2:35 PM), https://www.echr.coe.int/Documents/Convention_ENG.pdf
(142) Giancario Frosio, The European Court Of Human Rights Holds Delfi Liable For Anonymous Defamation, CENTRE FOR INTERNET AND SOCIETY STANFORD LAW SCHOOL (Feb 9, 2019, 2:49 PM), http://cyberlaw.stanford.edu/blog/2013/10/european-court-human-rights-holds-delfiee-liable-anonymous-defamation
(143) HUDOC - European Court of Human Rights, HUDOC (Feb 10, 2019, 6.25PM), http://hudoc.echr.coe.int/eng?i=001-126635#{"itemid":["001-126635"]
(144) Application no. 22947/13

ful comments from readers. In response, the real estate company sued MTE and Index for infringing its right to a good reputation. The Hungarian courts declined to apply the safe harbour principles under Directive 2000/31/EC, stating that the same applies only to commercial transactions of electronic nature i.e purchases made online. According to them the comments were made in a personal capacity and were outside the ambit of economic or professional undertakings, and hence not qualified for safe harbour protection.

The matter was moved to the European Court of Human Rights (ECHR). In a 2016 ruling that was considered an enormous step forward for protection of intermediary from liability and online free speech, the Court held that requiring intermediaries to regulate content posted on their platform *"amounts to requiring excessive and impracticable forethought capable of undermining freedom of the right to impart information on the Internet.*[145]" The Court also declared that the rulings of the Hungarian courts were against Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms.[146]

6.4 Right to Be Forgotten in the EU

The GDPR came into force on May 25, 2018, repealing the 1995 Data Protection Directive. It is meant to harmonize data privacy laws across Europe, protect data privacy of EU citizens and provide a comprehensive data privacy framework for organizations that collect and process data.[147]

Article 17 of the GDPR provides for the Right to Erasure or the Right to be Forgotten. This is a development from the Data Protection Directive (Directive 95/46/ec) where there was no mention of this term, although it was implicit under Articles 12 and 14. The grounds under Article 17 of the GDPR are detailed and broader than those provided in the 1995 Data Protection Directive. The data subject has the right to demand erasure of the information concerning her in the following cases:

- personal data is not required for processing;
- she withdraws consent;
- when there has been unlawful processing of data;
- objection is on grounds under Article 21(1) and Article 21(2) of GDPR;[148]
- national laws require erasure of data and; and
- when the data is provided in relation to information society services by a child under Article 8(1).[149]

The Article also provides for situations in which the Right to be Forgotten will not be applicable. The grounds are:

- exercise of the right of freedom of expression and information;
- public interest and public health;
- when the processing is a legal obligation;
- for archiving purposes with respect to public interest, scientific, historical research, or statistical purposes; and
- exercise or defence of legal claims.

However, RTBF under the GDPR is plagued with several problems, namely:

- Disproportionate Incentives: The infrastructure in place for Right to be Forgotten is

---

(145) Daphne Keller, New Intermediary Liability Cases from the European Court of Human Rights: What Will They Mean in the Real World? STANFORD LAW SCHOOL- CENTER FOR INTERNET AND SOCIETY (Feb 18, 2019, 6:20PM), http://cyberlaw.stanford.edu/blog/2016/04/new-intermediary-liability-cases-european-court-human-rights-what-will-they-mean-real

(146) Council of Europe, European Convention on Human Rights, EUROPEAN COURT OF HUMAN RIGHTS (9 Mar, 2019, 2:35 PM), https://www.echr.coe.int/Documents/Convention_ENG.pdf

(147) The European Union General Data Protection Regulation, (9 Mar, 2019, 2:49 PM), http://www.eugdpr.org/

(148) European Commission, Article 21 - Right to Object, EUROPEAN COMMISSION (9 Mar, 2019, 2:55 PM), http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

(149) European Commission, Article 8 - Conditions Applicable to Child's Consent in Relation to Information Society Services, EUROPEAN COMMISSION (9 Mar, 2019, 2:58 PM), http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

heavily tilted toward Right to Privacy and not toward informational rights and freedom of speech and expression. It provides unbalanced incentives to the Controller, thereby causing them to over comply and favour delisting in order to protect themselves. Article 83(5) provides fines as high as upto EUR 20,000,000, or in the case of an undertaking, upto 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. The Google Transparency Report which provides anonymized data on Right to be Forgotten requests has in its statistics, which began from May 29, 2014, stated that out of all the URLs they have evaluated for removal, 44.2% have been removed until February 2019.[150]

- Procedural Problems: According to both, the Google-Spain ruling and the GDPR, search engines are the initial adjudicators before whom data subjects file RTBF requests. This is similar to the intermediary liability takedown procedure and the same difficulties arise in this case as these questions involve a delicate balance between rights and private companies should not be the entities who make this determination. Publishers generally do not to have the right to approach courts under the GDPR regime. This leads to a clear tilt in the system towards the rights of the data subject's privacy rather than the freedom of speech and expression of the content writer or the publisher.[151]

- Hosting Platforms as Controllers: While it is settled that search engines are Controllers, there exists a lack of clarity on whether hosting platforms will have RTBF obligation on user content. This has not been resolved by the 2016 Resolution. It is probable that hosting platforms will process Right to be Forgotten requests to avoid liability and the risk of being included in the definition of Controller with all the obligations which come along with it.

- Applicability of E-commerce Directive[152] on Intermediaries: Article 2(4) of the GDPR states that the GDPR would be applicable without prejudice to the 2000 E-commerce directive, in particular Article 12 to 15 which pertain to intermediary liability. Often Intermediaries face dual liability under both data protection laws and intermediary liability laws where exists potential for such overlap.

6.5 EU cases on Right to Be Forgotten

6.5.1 Google v. Spain [153] (2014)

The landmark case of Google v. Spain before the Court of Justice of the European Union read in the Right to be forgotten from Articles 12 and 14 of the Data Protection Directive specifically with respect to delisting of search results by search engines, and laid down several important principles in this regard. The complainant in this case, one Mr. Costeja Gonzalez filed a case against Google for showing search results related to the auction of his property for recovery of social security debts, that took place ten years ago and was published in the Spanish newspaper La Vanguardia. He wanted the search engine to delist these links from the search engine as it was no longer relevant and harmed his reputation.

The following questions arose during the proceedings of the case:

(1) Whether search engines are 'Processors/ Controllers' of data?
Google stated that it is neither the Processor nor the Controller of data. It is not the Processor as it does not discriminate between personal data and general data while undertaking its activities and as it does not exercise any control over the data, it is not the

(150) Search Removals under European Privacy Law, Google Transparency Report, GOOGLE (March 1, 2019, 2:00PM), https://transparencyreport.google.com/eu-privacy/overview?hl=en
(151) Daphne Keller, The Right Tools: Europe's Intermediary Liability Laws and the 2016 General Data Protection Regulation, STANFORD LAW SCHOOL CENTER FOR INTERNET AND SOCIETY (fEB 9, 2019, 4:56PM) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2914684
(152) Electronic Commerce Directive 2000/31/EC
(153) [C-131/12]

Controller.[154] The Court, however, rejected this reasoning. Google was held to collect, record, retrieve, organize, store, disclose and make data available to the public, which comes under the definition of processing. The fact that the data is already published and not altered makes no difference.[155] The Court also held that because the search engine exercises control and determines the purpose and means of the activities that it undertakes during processing, it will be the Controller with respect to these activities and cannot be excluded only on the basis that it exercises no control over the personal data on the website of third parties. The Court also emphasized that entering a person's name into a search engine and getting all information pertaining to that person would enable profiling of that individual. [156] It was held that it is irrelevant that publishers possess the means to block search engines from accessing their data. The duty on search engines was separate from that of publishers of data.[157]

(2) What are the duties on the search engine operator as per the 1995 Data Protection Directive?

Google stated that as per the principle of proportionality, the publishers of the websites must take a call on whether the information should be erased or not as they are in the best position to make this determination and take further action for removal of such information. Google further contended that its fundamental right to free speech and expression along with that of the Publisher will be negatively affected if it is asked to delist such links. Additionally, informational rights of Internet users will also be under threat.

The Court once again emphasized the role of search engines in profiling of data subjects and the threat it poses to the right to privacy of individuals. The court further explained that the processing of data cannot be justified solely by the economic interests of the search engine. The rights of other Internet users are also to be considered. The rights of the data subject and that of other Internet users must be balanced by considering factors such as nature of information, sensitivity of the data in the data subject's life, the role of the data subject in public life and public interest.[158] The court also noted that because of ease in replication of data on the Internet, it may spread to websites over which the court does not have jurisdiction. Due to this, it may not be an effective remedy to mandate that there be parallel erasure of the data from both the publisher or to require erasure of data from the publisher's website first. There may also be situations where the data subject has the Right to be Forgotten against the search engine but not the publisher (Eg: If the data is solely for journalistic purpose[159]).

(3) Scope of data subjects rights under the Data Protection Directive

The question referred to the court was whether the data subject can exercise his Right to be Forgotten on the grounds that the data is prejudicial or that he wishes that the data be deleted after a reasonable time.

Google submitted that it is only in cases where the processing violates the Data Protection Directive or on compelling legitimate grounds particular to the data subject's situation that the individual be allowed to exercise the Right to be Forgotten.

The Court held that data collected could be lawful initially, but, may, in the course of time become irrelevant, inaccurate, inadequate, excessive with respect to the purpose

---

(154) Para 22 of the Google Spain vs AEPD and Mario Costeja Gonzalez decision
(155) Id. at Paras 28, 29
(156) Id. at Para 37
(157) Id. at Paras 39, 40
(158) Id. at Para 81
(159) Id. at Paras 84, 85

for which it was collected.[160] The Court also stated that it is not necessary that the data sought to be erased has to be prejudicial to the data subject.[161]

6.5.2 Google v. Equustek[162] (2017)

In 2011(Canada), Equustek Solutions Inc. filed a lawsuit against its distributor, Datalink Technologies, claiming that Datalink illegally obtained Equustek's trade secrets and other confidential information. Thereafter, Datalink allegedly began to pass off Equustek's products as its own by re-labelling them, and also started selling competing products by using Equustek's trade secrets. In response to this, Equustek procured several interlocutory injunctions against Datalink. However, Datalink disregarded the orders and moved its jurisdiction to some other location and continued its business.

In 2012, Equustek requested Google to de-index Datalink's websites from appearing on Google's search results. As a result, Google voluntarily blocked more than three hundred web pages from Google Canada but refused to do the same on an international scale.

The matter came up before the British Columbia Supreme Court, which, consequently, ruled that Google has to remove all of Datalink's web domains from its global search index. This was essentially a global takedown order. Google appealed the order in the Supreme Court of Canada, contending that the order was against the right to freedom of speech and expression. In a landmark 7-2 ruling, the Supreme Court upheld the lower court's worldwide takedown order, that required Google to delist Datalink's websites and domains from its global search index.

The ruling has received widespread criticism from various civil rights organizations and Internet advocates for violating the free speech rights of Internet users. Also, the question that arose was whether a country can enforce its laws in other countries to limit speech and access to information.

6.5.3 Google, Inc v. Commission nationale de l'informatique et des libertés (CNIL)[163] (2018)

Google was once again involved in a long legal wrangle; this time with the French data protection authority, Commission nationale de l'informatique et des libertés, commonly referred to as CNIL.

In this case, CNIL had ordered Google to delist certain items from its search results. Google had complied with the order, and delisted the concerned articles from its domains in the European Union (google.fr, google.de, etc). The delisted results, however, were still available on the ".com" and non European extensions. Subsequently, in May 2015, a formal injunction was issued against Google by the CNIL chair, ordering the search engine to extend delisting to all "Google Search" extensions within a period of fifteen days.[164] On failure to comply with the injunction order, Google was asked to pay a fine of EUR 10,000.

Google appealed the order in France's highest administrative court, Couseil d'Etat, and contended that the right to censor web results globally will seriously impair freedom of speech and expression and the right to access information. It was also argued that French authorities have no right to enforce their order worldwide, and doing so would set a dangerous precedent for other countries.

The French court referred the case to Europe's highest court, Court of Justice of the European Union (CJEU) for answers to certain legal questions and to arrive at a preliminary ruling before coming to a judgment on the case itself. Arguments were heard in September, 2018

---

(160) Id. at Para 93
(161) Id. at Para 99
(162) 2017 SCC 34
(163) [C-507/17]
(164) Right to be delisted: the CNIL Restricted Committee imposes a €100,000 fine on Google, CNIL(Feb 12, 2019, 3PM), https://www.cnil.fr/en/right-be-delisted-cnil-restricted-committee-imposes-eu100000-fine-google

and judgement is awaited.

The Court published the Advocate General's opinion in January, which stated that de-referencing search results on a global basis will under freedom of speech and expression:[165]

"[T]here is a danger that the Union will prevent people in third countries from accessing information. If an authority within the Union could order a global deference, a fatal signal would be sent to third countries, which could also order a dereferencing under their own laws. … There is a real risk of reducing freedom of expression to the lowest common denominator across Europe and the world."

Google v. CNIL highlights the incompatibility between principles of territorial jurisdiction and global data flows.[166]

(165) 'Right to be forgotten' by Google should apply only in EU, says court opinion, THE GUARDIAN (Feb 8, 2019, 7:08PM), https://www.theguardian.com/technology/2019/jan/10/right-to-be-forgotten-by-google-should-apply-only-in-eu-says-court

(166) Michele Finck, Google v CNIL: Defining the Territorial Scope of European Data Protection Law, THE GUARDIAN (Feb 7, 2019, 2:00PM), https://www.theguardian.com/technology/2019/jan/10/right-to-be-forgotten-by-google-should-apply-only-in-eu-says-court

CHAPTER VII

FAKE NEWS AND SOCIAL MEDIA: WHO IS RESPONSIBLE?

Social media and messaging platforms provide the perfect condition for the creation of cascades of information of all kinds. The power of these platforms has been leveraged to create social movements like Black Lives Matter, MeToo and TimesUp campaigns. This power has also been exploited to sow discord and manipulate elections.

The emergence of social media saw shifts in the media ecosystem with Facebook and Twitter becoming important tools for relaying information to the public. Anyone with a smartphone can be a broadcaster of information. Political parties are investing millions of dollars on research, development and implementation of psychological operations to create their own computational propaganda campaigns.[167] The use of automated bots to spread disinformation with the objective of moulding public opinion is a growing threat to the public sphere in countries around the world.[168] This raises new concerns about the vulnerability of democratic societies to fake news and the public's limited ability to contain it.[169]

Fake news[170] is not a recent phenomenon. The issue of disinformation has existed since time immemorial in both traditional print and broadcast media. The advent of the Internet during the 90s opened the doors to a vast repository of information for people. The unimaginable growth of the Internet in a few years made it a host for a plethora of false and unwanted information. The World Economic Forum in 2013 had warned that 'digital wildfires' i.e unreliable information going viral will be one of the biggest threats faced by society and democracy: *"The global risk of massive digital misinformation sits at the centre of a constellation of technological and geopolitical risks ranging from terrorism to cyber attacks and the failure of global governance".*[171]

---

(167) Philip N. Howard, Samantha Bradshaw, The Global Organization of Social Media Disinformation Campaigns, COLUMBIA JOURNAL OF INTERNATIONAL AFFAIRS (Mar 2, 2019, 3:09PM) https://jia.sipa.columbia.edu/global-organization-social-media-disinformation-campaigns

(168) Dean Jackson, How Disinformation Impacts Politics and Publics, NATIONAL ENDOWMENT FOR DEMOCRACY (Feb 7, 2019, 12:30PM) https://www.ned.org/issue-brief-how-disinformation-impacts-politics-and-publics/

(169) David Lazer, Matthew Baum, Nir Grinberg, Lisa Friedland, Kenneth Joseph, Will Hobbs, Carolina Mattsson, Combating Fake News: An Agenda for Research and Action, HARVARD KENNEDY SCHOOL, SHORENSTEIN CENTER (Feb 10, 2019, 7:56PM), https://shorensteincenter.org/combating-fake-news-agenda-for-research/

(170) In this report, the term "Fake News" refers to news that is deliberately and verifiably false and created with the intention to mislead readers.

(171) Lee Howell, Global Risks, Insight Report, WEF, 23 (2013)

In the 2016 United States Presidential elections[172] and the 2018 Brazilian Presidential elections,[173] the power of social media and messaging platforms was leveraged to sway elections in the favour of a particular candidate. The incidents commenced a global debate on tackling fake news and whether tech platforms are complicit in the issue. In the wake of these controversial elections there has been mounting pressure on online platforms such as Facebook and Twitter to actively regulate their platforms.

Governments around the world have been grappling with the question of how existing laws that limit free speech for reasons such as incitement to violence can be applied in the digital sphere.[174] Increasing calls for the platforms to take a more proactive role in weeding out disinformation and hate speech have raised fears that they might become the ultimate arbiters of what constitutes unacceptable content.[175]

India has been reeling from the consequences of fake news floating on social media and messaging platforms, especially WhatsApp that has more than 200 million active Indian users.[176] Rumours related to possession of beef and child kidnapping have led to the deaths of thirty three innocent people.[177] BBC conducted a research in India on the cause and motivation behind the viral dissemination of fake news. The study found that the rising tide of nationalism along with a distrust in mainstream media has pushed people to spread information from alternative sources without attempting to verify the information, under the belief that they were helping to spread a real story.[178]

Following the spate of mob lynchings, the Indian Government asked WhatsApp to devise ways to trace the origin of fake messages circulated on its platform.[179] The government cautioned WhatsApp that it cannot evade responsibility if its services are being used to spread disinformation and will be treated as an "abettor" for failing to take any action.[180]

In India, as mentioned in chapter, the Draft Information Technology [Intermediaries Guidelines (Amendment) Rules], 2018 ("Draft Rules") have been proposed by the government to fight 'fake news', terrorist content and obscene content, among others. They place obligations on intermediaries to proactively monitor content uploaded on their platforms and enable traceability to determine the originator of information.

The Election Commission of India announced that all candidates contesting the 2019 general elections will have to submit details of

---

(172) Richard Gunther, Paul A. Beck, Erik C. Nisbet, Fake News Did Have a Significant Impact on the Vote in the 2016 Election, OHIO STATE UNIVERSITY, https://cpb-us-w2.wpmucdn.com/u.osu.edu/dist/d/12059/files/2015/03/Fake-News-Piece-for-The-Conversation-with-methodological-appendix-11d0ni9.pdf

(173) Anthony Broadle, Explainer: Facebook's WhatsApp flooded with fake news in Brazil election, REUTERS (Feb 19, 2019, 4:07PM), https://in.reuters.com/article/brazil-election-whatsapp/explainer-facebooks-whatsapp-flooded-with-fake-news-in-brazil-election-idINKCN1MV04J

(174) Lee Howell, Global Risks, Insight Report, WEF, 23 (2013)

(175) Platform responsibility, The London School of Economics and Political Science, Department of Media and Communications, LSE (Mar 4, 2:09PM) http://www.lse.ac.uk/media-and-communications/truth-trust-and-technology-commission/platform-responsibility

(176) WhatsApp now has 1.5 billion monthly active users, 200 million users in India, FINANCIAL EXPRESS (Dec 11, 2018, 5:06PM), https://www.financialexpress.com/industry/technology/whatsapp-now-has-1-5-billion-monthly-active-users-200-million-users-in-india/1044468/

(177) Alison Saldanah, Pranav Rajput, Jay Hazare, Child-Lifting Rumours: 33 Killed In 69 Mob Attacks Since Jan 2017. Before That Only 1 Attack In 2012, INDIA SPEND (Feb 5, 2019, 11:40AM), https://www.indiaspend.com/child-lifting-rumours-33-killed-in-69-mob-attacks-since-jan-2017-before-that-only-1-attack-in-2012-2012/

(178) Santanu Chakrabarti, Lucile Stengel, Sapna Solanki, Duty, Identity, Credibility: Fake News and the Ordinary Citizen in India, BBC (Feb 5, 2019, 11:45AM), http://downloads.bbc.co.uk/mediacentre/duty-identity-credibility.pdf

(179) PTI, Mob Lynchings: WhatsApp At Risk Of Being Labelled "Abettor", BLOOMBERG QUINT (Feb 1, 2019, 10 AM), https://www.bloombergquint.com/law-and-policy/mob-lynchings-whatsapp-at-risk-of-being-labelled-abettor#gs.UdkfqXqo

(180) Id

their social media accounts and all political advertisements on social media will require prior certification.[181] All expenditure of campaigning on social media is to be included in the candidates election expenditure disclosure.[182]

The growing pressure worldwide on intermediaries to implement gatekeeping policies led Germany to pass "Netzwerkdurchsetzungsgesetz" (NetzDG), also known as the Network Enforcement Act, which requires social networks with more than 2 million users to take down content that is "obviously illegal" within 24-hours after it is notified.[183] The law imposes fines of up to EUR 50 million on social media companies that fail to remove unlawful content from their websites.

In its latest transparency report[184] on removals under the NetzDG, Google stated that it received 465,784 requests in 2018 from users and reporting agencies to remove undesirable content from YouTube. The reasons provided for the complaints include: privacy, defamation, hate speech, political extremism, sexual content, terrorism-related and unconstitutional content, amongst others. In response to the removal requests, 112,941 items were removed by Google. Facebook, in its NetzDG Transparency Report, mentioned that it received 1,386 removal requests identifying a total of 2,752 pieces of content between Jan-Dec, 2018.[185]

In 2018, the French Parliament passed a controversial legislation that empowers judges to order the immediate removal of "fake news" during election campaigns. The law allows the French national broadcasting agency to render the authority to suspend television channels "controlled by a foreign state or under the influence" of that state if they "deliberately disseminate false information likely to affect the sincerity of the ballot.[186]

The European Commission and four major social media platforms - Facebook, Twitter, YouTube and Microsoft announced a Code of Conduct on countering illegal online hate speech.[187] The Code met with opposition from a number of rights groups like Index of Censorship[188] and EFF for being in violation of the fundamental right to freedom of expression.[189] The Code of Conduct is part of a trend where states are pressuring private corporations to censor content without any independent adjudication of the legality of the content.[190]
After the Cambridge-Analytica debacle, the Honest Ads Act was introduced in the United States Senate which would hold social media and other online platforms to the same political advertis-

(181) Scroll Staff, Lok Sabha polls: All political ads on social media will need prior certification, says ECI, SCROLL (Mar 7, 2019, 2:30PM), https://scroll.in/latest/916091/lok-sabha-polls-all-political-ads-on-social-media-will-need-prior-certification-says-eci
(182) Nikhil Pahwa, Key takeways from Election Commission's 2019 India's 2019 Elections announcement: On Fake News, Online Political Advertising and Model Code of Conduct, MEDIANAMA (Mar 8, 12:30PM), https://www.medianama.com/2019/03/223-key-takeways-from-election-commissions-2019-indias-2019-elections-announcement-on-fake-news-online-political-advertising-and-model-code-of-conduct/
(183) BBC, Germany starts enforcing hate speech law, BBC (Feb 4, 2019, 11:30AM) https://www.bbc.com/news/technology-42510868
(184) Removals under the Network Enforcement Law, Google Transparency Report, GOOGLE (Jan 4, 2019, 11:05AM), https://transparencyreport.google.com/netzdg/youtube?hl=en
(185) NetzDG Transparency Report, FACEBOOK (Jan 4, 2019, 11:05AM), https://fbnewsroomus.files.wordpress.com/2018/07/facebook_netzdg_july_2018_english-1.pdf
(186) Michael-Ross Florentino, France passes controversial 'fake news' law, EURONEWS (Mar 2, 2019, 2:30PM) https://www.euronews.com/2018/11/22/france-passes-controversial-fake-news-law
(187) Code of Conduct on countering online hate speech – results of evaluation show important progress, EUROPEAN COMMISSION (Mar 2, 2019, 2:40PM) https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=71674
(188) EU agreement with tech firms on hate speech guaranteed to stifle free expression, INDEX ON CENSORSHIP (Mar 2, 2019, 1:20PM) https://www.indexoncensorship.org/2016/05/eu-agreement-tech-firms-hate-speech-guaranteed-stifle-free-expression/
(189) Jillain York, European Commission's Hate Speech Deal With Companies Will Chill Speech, EFF (Mar 7, 2019, 3:02PM), https://www.eff.org/deeplinks/2016/06/european-commissions-hate-speech-deal-companies-will-chill-speech
(190) Responding to 'hate speech': Comparative overview of six EU countries, ARTICLE 19 (Mar 3, 2019, 6:00PM) https://www.article19.org/wp-content/uploads/2018/03/ECA-hate-speech-compilation-report_March-2018.pdf

ing transparency requirements that bind cable and broadcast systems.[191] The bill would require companies to disclose how advertisements were targeted as well as how much they cost.92[192]

While governments are struggling to implement regulations that would address the significant challenge of combating the rising instances of fake news without jeopardising the right to free expression, there are difficult questions that arise: What should be the extent to which limits on free speech online should be imposed so that the utility of the Internet is not compromised? Does today's digital capitalism make it profitable for tech companies to circulate click-worthy narratives?[193] Would regulating intermediaries without addressing the deeper and structural issues of lack of user education and media literacy be enough to solve the problem?

In 2017, in a 'Joint declaration on freedom of expression and 'Fake News', disinformation and propaganda', United Nations Special Rapporteur on Freedom of opinion and expression, David Kaye, stated that *"General prohibitions on the dissemination of information based on vague and ambiguous ideas, including "false news" or "non-objective information", are incompatible with international standards for restrictions on freedom of expression, and should be abolished."*[194]

The UK House of Commons, Digital, Culture, Media and Sports Committee in its final report on disinformation and fake news recommended that digital literacy should be the fourth pillar of education, alongside reading, writing and maths. An educational levy can be raised on social media companies to finance a comprehensive educational framework—developed by charities, NGOs, and the regulators themselves—and based online.[195]

It was also recommended that social media companies should be more transparent about their sites and how they work. Instead of hiding behind complex agreements, they should inform users about how their sites work, including curation functions and the way in which algorithms are used to prioritise certain stories, news and videos, depending on each user's profile.[196] The Committee advised the enactment of a compulsory code of ethics, overseen by an independent regulator which would have statutory powers to monitor tech companies.[197] On advertisements related to political campaigning, the Committee was of the view that the government should define 'digital campaigning' including online political advertising, and that paid political advertising should be publicly accessible, clear and easily recognisable.[198]

In January 2018, the European Commission set up a high-level group of experts to advise on policy initiatives to counter fake news and disinformation spread online.[199] The High Level Committee recommended enhancing transparency, promoting media and information literacy, developing tools for empowering users and journalists, safeguarding the diversity and sustainability of the news media ecosystem and promoting continued re-

(191) Ellen P. Goodman, Lyndsay Wajert, The Honest Ads Act Won't End Social Media Disinformation, but It's a Start, SSRN, (2017)
(192) Jack Nicas, Facebook to require verified identities for future political ads, NYTIMES (Mar 2, 2019, 2:50PM) https://www.nytimes.com/2018/04/06/business/facebook-verification-ads.html
(193) Evgeny Morozov, Moral panic over fake news hides the real enemy – the digital giants, The Guardian, (Jan 4, 2019, 10 AM), https://www.theguardian.com/commentisfree/2017/jan/08/blaming-fake-news-not-the-answer-democracy-crisis
(194) David Kaye, Freedom of Expression Monitors Issue Joint Declaration on 'Fake News', Disinformation and Propaganda, OHCHR (Mar 2, 2019, 5:00PM) https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21287&LangID=E
(195) Disinformation and'fake news': Final Report, House of Commons Digital, Culture, Media and Sport Committee, UK PARLIAMENT (Mar 3, 2019, 1:52PM), https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/179102.htm
(196) Id.
(197) Id.
(198) Id.
(199) A multi-dimensional approach to disinformation, Report of the independent High level Group on fake news and online disinformation, EUROPEAN COMMISSION (Mar 2, 2019, 8:10PM), https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation

search on the impact of disinformation.[200]

Oliver Sylvain in Connecticut Law Review proposes that courts should scrutinize the manner in which each website elicit user content and the extent to which they exploit that data in secondary or ancillary markets. Based on that, the level of protection under the intermediary liability legal regime should be decided, depending on whether a particular provider qualifies as an active or passive intermediary.[201]

Governments should enact a regulatory framework that ensures accountability and transparency of digital platforms without curbing free speech and innovation. The answer to bad speech should not be censorship. Such a regulatory framework should be developed as a result of multi-stakeholder consultations that involves the government, legal community, tech companies, civil society and regular users of social media.

7.1 Multi-stakeholder Perspectives on Combating Fake News

SFLC.in conducted a series of discussions on fake news and intermediary liability across India in January 2019 including New Delhi (Jan 11, 18 and Feb 13), Bengaluru (Jan 15), Mumbai (Jan 16),Kochi (Jan 30), Hyderabad (Feb 12).[202]

Some of the key findings from the discussions are:

- The definition of 'fake news' is vague and ambiguous and has to be deconstructed. There is no real agreement as to what the expression means. It is being used in an elastic manner and is being brandished as an all purpose slogan to describe everything from errors to deliberate falsehoods. World leaders have been seen weaponizing this term and using it against news organizations and journalists whose coverage they find disagreeable.

It was agreed that the best way to understand the term Fake News is to deconstruct it into three terms: misinformation, disinformation and malinformation. Misinformation was construed as circulation of incorrect information without any bad intention, Malinformation was defined as spread of real information to cause harm to a person, organization or society. Disinformation was understood to be false narrative deliberately spread to inflict harm.

- Information diet is coming from algorithms on social media platforms. There is a real problem of filter bubbles on these platforms. Therefore, it is important to think about algorithmic transparency and algorithm accountability.

- Regarding deployment of artificial intelligence, industry experts dealing with AI on a regular basis claimed that AI was nowhere near being ready for the task of solving human and political problems.

- Fact checking must be the foundation of journalism. There are very few independent fact checkers in India. After verifying the facts of a particular story, the next step must be to put the fact checked story back on the platform it emanated from and make it as viral as the fake news. It has to be packaged in a manner similar to the fake news with catchy / clickbait headlines. The government must encourage and empower independent journalism which is the backbone of a democratic setup.

- Vernacular media sources are witnessing higher viewership compared to English media. Navbharat Times, one of the largest circulated Hindi newspapers is progressing towards highest online subscribers. However, fact-checking is limited to English media only. There is a lack of incentives to fact-checkers in advertisement based business models of online media groups.

- Social media giants should scale up their

---

(200) Id.
(201) Olivier Sylvain, Intermediary Design Duties, 50, CONNECTICUT LAW REVIEW, 1 (2018)
(202) Blue Paper: Misinformation and Intermediary Liability, SFLC.in (Mar 1, 2019, 2:45PM), https://sflc.in/blue-paper-misinformation-and-draft-intermediary-guidelines/

efforts to fact check and down-rank information proliferating on their platforms by collaborating with third party fact checkers.

- There is a problem in the education system. Apart from digital literacy, there is a need to teach critical thinking skills to young people. A culture of questioning and skepticism should be encouraged.

- Decentralization of technology is important to break information monopolies.

- Other suggested solutions included providing incentives to startups that do fact checking, giving tax breaks to small organizations that bring truth back as an important value in the digital realm.

- The proposed Draft Rules can act like a minesweeper and have the potential to be misused. Regulation should be such that it aids in the growth of a free Internet instead of restricting it.

While digital and media literacy is indispensable in ensuring that consumers of information on social media do not fall prey to disinformation, we cannot dismiss the roles that tech companies should play in addressing the issue by ramping up their efforts to keep their platforms clean. Platforms should expand their endeavours to work jointly with third party fact checkers and invest in educating users and developing tools to help them distinguish between news that comes from a reliable source and stories coming from outlets that are regarded as unreliable. WhatsApp recently limited forwarding messages to five chats to contain the virality of messages on their platform.[203] The messaging platform launched TV and Radio campaigns to spread awareness[204] and partnered with local NGOs to educate users about the need to verify information.[205]

Facebook is working with their community and third-party fact-checking organizations to identify false/fake news and limit the spread. Ahead of the General Elections 2019, Facebook has partnered with seven third party fact-checkers namely: BOOM-Live, AFP, India Today Group, Vishvas.news, Factly, Newsmobile and Fact Crescendo covering six languages, to review and rate the correctness of stories on Facebook.[206] The platform is also in the process of setting up an operations centre in Delhi which would be responsible to monitor election content 24X7. To achieve this, the centre will be coordinating with global Facebook offices located at Menlo Park (California), Dublin and Singapore.[207]

Facebook has devised new features to bring more transparency in advertisements on its platform in India.[208] The platform will allow its users to view the publishers and sponsors of the advertisement they are accessing.[209] It has rolled out a searchable ad library for its viewers to analyze political ads. The information provided by this ad library includes range of impressions, expenditure on the said ads and the demographics of who saw the ad.[210]

Any efforts to label and identify questionable stories or sources should be consistent

---

(203) WhatsApp Blog, More changes to forwarding, WHATSAPP (Mar 2, 2019, 5:40PM), https://blog.whatsapp.com/10000647/More-changes-to-forwarding

(204) PTI, WhatsApp rolls out TV campaign in India to tackle fake news, LIVEMINT (Mar 2, 2019, 5:40PM), https://www.livemint.com/Companies/QU7LWGcHf0m49uiBqDRzlN/WhatsApp-rolls-out-TV-campaign-in-India-to-tackle-fake-news.html

(205) WhatsApp embarks on user-education drive to curb fake messages, HINDU BUSINESS LINE (Mar 2, 2019, 6:00PM), https://www.thehindubusinessline.com/news/whatsapp-embarks-on-user-education-drive-to-curb-fake-messages/article24812353.ece

(206) Nandita Mathur, Facebook planning a 'war room' in Delhi to monitor Elections 2019, LIVE MINT, (8th March 2019, 12:20 PM), https://www.livemint.com/elections/lok-sabha-elections/facebook-wants-to-set-up-a-war-room-in-delhi-to-monitor-elections-2019-1552246631884.html

(207) Id.

(208) Shivnath Thukral, Bringing More Transparency to Political Ads in India, (8th March 2019, 12:50 PM), https://newsroom.fb.com/news/2018/12/ad-transparency-in-india/

(209) Id.

(210) Id.

across platforms.[211] Voters should be able to identify untrustworthy content across platforms and trust that all platforms use the same standards to classify it.[212]

Transparency about algorithms, content moderation techniques and political advertising will go a long way in countering the problem.[213] Large social media platforms are generally founded on the economic model of surveillance capitalism rooted in delivering advertisements based on data collection.[214] Decentralized, user owned, free and open source platforms that do not rely on widespread data collection can potentially limit the spread of fake news.[215]

It is short-sighted to think that laws can completely fix the problem, it is nevertheless necessary to have a discussion about a regulatory framework that ensures accountability and transparency of digital platforms without curbing free speech and innovation. The answer to bad speech should not be censorship. Such a regulatory framework should be developed as a result of multi-stakeholder consultations that involves the government, legal community, tech companies, civil society and regular users of social media.
The objective of the Draft Information Technology [Intermediaries Guidelines (Amendment) Rules], 2018 ("the Draft Rules") seems to be to counter disinformation / fake news on social media and messaging platforms but its purpose will not be served by such arbitrary and sweeping provisions. The Draft Rules are violative of the fundamental rights to free speech and privacy and the dictum of the judgment of the Supreme Court in Shreya Singhal v Union of India. While transparency and accountability of platforms is the need of the hour, the government should enact a less-invasive and proportional means of regulation of the internet.

(211) Abby K. Wood, Ann M. Ravel, Fool Me Once: Regulating "Fake News" and other Online Advertising, 1227, SOUTHERN CALIFORNIA LAW REV., 55 (2018)
(212) Id.
(213) Matteo Monti, Perspectives on the Regulation of Search Engine Algorithms and Social Networks: The Necessity of Protecting the Freedom of Information, 1, OPINIO JURIS IN COMPARATIONE, 10 (2017)
(214) Natasha Singer, The Week in Tech: How Google and Facebook Spawned Surveillance Capitalism, NYTIMES (Mar 1, 2019, 8:30PM), https://www.nytimes.com/2019/01/18/technology/google-facebook-surveillance-capitalism.html
(215) Mark Verstraete, Derek E. Bambauer, Jane R. Bambauer, Identifying and Countering Fake News, Discussion Paper 17-15, ARIZONA LAW JOURNAL, 25 (2017)

CHAPTER VIII

OBSERVATIONS AND CONCLUSION

Increase in the number of users of online platforms that allow sharing of user generated content coupled with a lack of media literacy have led to an explosion of harmful content ranging from hate propaganda to disinformation to revenge porn and child pornography. Targeted messages aimed at manipulating democratic processes as seen in the 2016 US Presidential election and the 2018 Brazil elections led to greater scrutiny of the accountability of platforms over user generated content, often focusing on the technology rather than systematic interventions.

Platforms like Facebook are no longer passive players like blogging platforms or web hosts and they decide the reach of content and ranking. What users see on their feeds are determined by their past browsing habits and their posts and shares. Thus, platforms have a major role to ensure that their platforms are safe and that the spread of disinformation is contained. The initiative of intermediaries in working together with fact checkers across the world is a positive move and will improve the trust of users in the content shared.

Although law is often said to be lagging technology, recent developments have shown that content platforms were slow in identifying the root causes that led to the rise of disinformation on the platforms. Intermediaries could have been faster to react to the problem of harmful messages on their platforms which led to harm in the offline world including incidents of physical violence. This inaction has contributed to a decrease in trust of users on the platforms in the recent past.

The trust deficit of online platforms and incidents attributed to harmful content spread online have been used by Governments in various countries as excuses to justify new regulations that seek to control information on these platforms. Whether it is NetzDG law in Germany or mandatory back-doors as per the new Australian law or the proposed amendment to the Intermediary Rules in India, the underlying narrative has been the need to control harmful content spread on social media platforms.

In India, the *Shreya Singhal* judgment has given intermediaries the much needed certainty on the requirements for enjoying

safe-harbour protection. However, the proposed amendments to the Intermediaries Guidelines Rules endangers this protection. Attempts at regulating intermediaries by weakening encryption or by mandating automated take-down on a broad range of content deemed to be harmful will be counterproductive and will affect the fundamental rights of free speech and privacy guaranteed to citizens. However, a *laissez faire* approach permitting intermediaries complete freedom is also not advisable as the real-world harm caused by illegal content cannot be ignored.

Governments should be free to mandate intermediaries to ensure quick resolution of legitimate takedown requests and to have in place governance structures and grievance mechanisms to enable this.

Although intermediaries can explore technology solutions like Artificial Intelligence tools to flag harmful content, there should be more investments in human moderation. For a country like India with multiple languages and diverse cultures, AI tools have their limitations and platforms will have to invest in people and resources to make the online world a safe space.

Intermediaries need to show more commitment to keep the platforms safe and secure. The oversight board proposed by Facebook is a step in the right direction. However, there are no quick fixes to the enormous problem of harmful content.

Based on discussions with various stakeholders over a series of interviews and roundtables, the recommendations can be summarized as:

Recommendations for Government:

- Laws on intermediary liability should provide a clear guidance on type of content that is deemed to be illegal.
- The Notice and action procedure should protect the rights of users and should not be ambiguous.
- The law should mandate governance structures and grievance mechanisms on the part of intermediaries enabling quick take-down of content determined as illegal by the judiciary or appropriate Government agency.
- The right to privacy of users should be protected and there should not be any mandate forcing intermediaries to weaken encryption or provide back-doors.
- Government should work with Intermediaries to educate users on identifying disinformation and in secure use of the Internet.
- The Government should formulate training programmes on technology law for lower judiciary so that the developments in jurisprudence in this area are disseminated.

Recommendations for Intermediaries:

- Intermediaries should invest resources to ensure that their platforms are safe and secure for users.
- Technology including Artificial Intelligence has its limitations and there should be proper safeguards to ensure that automated tools do not lead to taking down of legitimate content.
- Governance structures and grievance redressal mechanisms have to be instituted to resolve legitimate requests from the judiciary and the Government.
- Intermediaries need to work closely with fact checkers and mainstream media to reduce spread of disinformation on their platforms. There should be greater investments on resources and human moderation to cover content in regional languages.
- There should be greater cooperation between intermediaries to flag extreme content like terrorist content and child pornography.
- The “filter bubble” effect where users are shown similar type of content results in users not being exposed to opposing views and debates resulting in them becoming easy targets of disinformation. Intermediaries should work on reducing the echo chamber effect so that posts that are flagged as disinformation do not become viral.

ANNEXURE

The Amendments and Additions made by the Draft Information Technology [Intermediaries Guidelines (Amendment) Rules], 2018

NO	Rule No.	IL Rules, 2011 ('Old Rules')	Draft IL Rules, 2018 ('Draft Rules')
1	Rule No. 2 (Definition Clause)	Did not contain the definition of the term 'Appropriate Government'.	Inserted the term 'Appropriate Government' to mean the same as under the IT Act.
2	Rule No. 2 (Definition Clause)	Did not contain the definition of the term 'Critical Information Infrastructure'.	Inserted the term 'Critical Information Infrastructure' to mean the same as per Sec. 70(1) of the IT Act.
3	Rule No. 3(2) (Terms and Conditions and Privacy Policy)	Rule 3(2) required intermediaries to publish rules and regulations; or terms and conditions; or user agreements to inform users about certain content.	The Draft Rules have inserted the term 'privacy policy' in place of 'terms and conditions' in this provision.
4	Rule No. 3(2) (Details to be mentioned in user agreements)	Contained sub-clauses (a) to (i), which enlists the types of content which users cannot share on the intermediary's platform. Such as, content which, inter alia, is - grossly harmful; harms minors; and infringes intellectual property.	The Draft Rules inserted clause (j) and (k), which bar information which - (a) threatens public health/ safety; (b) 'promotes' cigarettes/ tobacco products; (c) promotes consumption of intoxicant, including alcohol/ e-cigarettes/ and like products; and (d) threatens critical information infrastructure.
5	Rule No. 3(4) of the Old Rules and 3(8) of the Draft Rules	Rule Rule 3(4) required intermediaries to 'disable' information which was in contravention of parameters laid down in their user agreements/ terms and conditions [as per Rule 3(2)], upon obtaining knowledge themselves or by an affected person in writing. This provision required intermediaries to takedown content within 36 hours and also retain such information for 90 days to aid investigation.	The Draft Rules have deleted the language used in Rule 3(4) of the Old Rules and have inserted Rule 3(8) in place of it. According to the new Rule 3(8), intermediaries are required to takedown content only when instructed by a court or notified by the appropriate government or its agency. Such takedown requests need to adhere to the restrictions laid down in Art. 19(2) of the Indian Constitution. Intermediaries under the new provision are required to remove content 'as far as possible immediately' but in no case later than 24-hours of being intimated. The new provision also requires intermediaries to retain taken down content for 180 days or longer (as required).

NO	Rule No.	IL Rules, 2011 ('Old Rules')	Draft IL Rules, 2018 ('Draft Rules')
6	Rule No. 3(5) of the Old Rules and 3(4) of the Draft Rules	Rule 3(5) required intermediaries to intimate their users on their right to terminate access and remove non-compliant information for not adhering to their internal rules/ user agreements/ privacy policies.	Rule 3(4) of the Draft Rules (which replaces the old provision) now requires such intimation to be 'at least once every month'.
7	Rule No. 3(7) of the Old Rules and 3(5) of the Draft Rules	Rule 3(7) required intermediaries to provide information to government agencies who are lawfully authorised for investigative, protective and cyber security activity. The information under this provision could be sought for punishment of offences under any law in force. Such seeking of information by government agencies had to be in writing and clearly stating the purpose.	Rule 3(5) of the Draft Rules replaces Rule 3(7) and makes the following changes : a) Introduces a requirement to assist 'any government agency' within 72 hours of intimation; b) The written request by government agencies could also be through 'electronic means'; and c) Intermediaries need to enable 'tracing out of originator' of information on their platforms as required by government agencies, legally authorised.

Note: This table does not discuss the unchanged provisions from the earlier Intermediaries Guidelines from 2011.

66A (Now Repealed). Punishment for sending offensive messages through communication service, etc.
Any person who sends, by means of a computer resource or a communication device,—

(a) any information that is grossly offensive or has menacing character; or
(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device,
(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages,
shall be punishable with imprisonment for a term which may extend to three years and with fine.

Explanation.— For the purpose of this section, terms "electronic mail" and "electronic mail message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, images, audio, video and any other electronic record, which may be transmitted with the message.

67. Punishment for publishing or transmitting obscene material in electronic form.–Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

69. Power to issue directions for interception or monitoring or decryption of any information through any computer resource.–

(1) Where the Central Government or a State Government or any of its officers specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient so to do,in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may subject to the provisions of sub-section **(2)**, for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.

(2) The procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.

(3) The subscriber or intermediary or any person in-charge of the computer resource shall, when called upon by any agency referred to in sub-section (1), extend all facilities and technical assistance to–
(a) provide access to or secure access to the computer resource generating,transmitting, receiving or storing such information; or
(b) intercept, monitor, or decrypt the information, as the case may be; or
(c) provide information stored in computer resource.

(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with imprisonment for a term which may extend to seven years and shall also be liable to fine.

69A. Power to issue directions for blocking for public access of any information through any computer resource.–

(1) Where the Central Government or any of its officers specially authorised by it in this behalf is satisfied that it is necessary or expedient so to do,in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-section (2),for reasons to be recorded in writing, by order, direct any agency of the Government or intermediary to block for access by the public or cause to be blocked for access by the public any information generated, transmitted, received, stored or hosted in any computer resource.

(2) The procedure and safeguards subject to which such blocking for access by the public may be carried out, shall be such as may be prescribed.

(3) The intermediary who fails to comply with the direction issued under sub-section **(1)** shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine.

79. Exemption from liability of intermediary in certain cases.–(1) 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.
(2) The provisions of sub-section (1) shall apply if–
(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or

(b) the intermediary does not–
(i) initiate the transmission,
(ii) select the receiver of the transmission, and
(iii) select or modify the information contained in the transmission;

(c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

(3) The provisions of sub-section (1) shall not apply if–

(a) the intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of the unlawful act;

(b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

Explanation.–For the purposes of this section, the expression "third party information"means any information dealt with by an intermediary in his capacity as an intermediary.

SECTIONS OF THE COPYRIGHT ACT, 1957

51.When copyright infringed.— Copyright in a work shall be deemed to be infringed—
(a) when any person, without a licence

granted by the owner of the copyright or the Registrar of Copyrights under this Act or in contravention of the conditions of a licence so granted or of any condition imposed by a competent authority under this Act—
(i) does anything, the exclusive right to do which is by this Act conferred upon the owner of the copyright, or
(ii) 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; or

(b) when any person—
(i) makes for sale or hire, or sells or lets for hire, or by way of trade displays or offers for sale or hire, or
(ii) distributes either for the purpose of trade or to such an extent as to affect prejudicially the owner of the copyright, or
(iii) by way of trade exhibits in public, or
(iv) imports into India, any infringing copies of the work:

Provided that nothing in sub-clause (iv) shall apply to the import of one copy of any work for the private and domestic use of the importer.

Explanation.— For the purposes of this section, the reproduction of a literary, dramatic, musical or artistic work in the form of a cinematograph film shall be deemed to be an "infringing copy".

52. Certain acts not to be infringement of copyright.—
(1) The following acts shall not constitute an infringement of copyright, namely,—

(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 facilitation 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.

NOTES

sflc.in

ABOUT US:

SFLC.IN is a donor supported legal services organization that brings together lawyers, policy analysts, technologists, and students to protect freedom in the digital world. We promote innovation and open access to knowledge by helping developers make great Free and Open Source Software, protect privacy and civil liberties of citizens in the digital world through education and provision of pro bono legal advice, and help policy makers make informed and just decisions with the use and adoption of technology. Please feel free to contact us to learn more about protecting your rights in the online world.

INTERMEDIARY LIABILITY 2.0: A SHIFTING PARADIGM

K-9, Birbal Road, Second Floor, Jangpura Extension, New Delhi - 110014, India.
Tel: +91-11-43587126 Fax: +91-11-24320809
www.sflc.in