

PERSONAL DATA PROTECTION AND INTERMEDIARY LIABILITY:
A LEGAL STUDY

Dissertation submitted to National Law University and Judicial Academy, Assam

in partial fulfillment for award of the degree of

MASTER OF LAWS/

ONE-YEAR LL.M. DEGREE PROGRAMME

Submitted by

Utkarsh Singh

SM0221031

LL.M(2021-22) IInd SEM

Supervised by

Dr. Kailash Jeenger

Associate Professor of Law



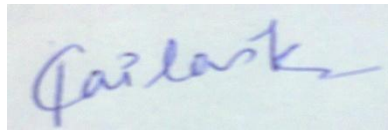
National Law University and Judicial Academy, Assam

July, 2022

CERTIFICATE

This is to certify that Utkarsh Singh has completed his dissertation titled “**PERSONAL DATA PROTECTION AND INTERMEDIARY LIABILITY:A LEGAL STUDY**” under my supervision for the award of the degree of MASTER OF LAWS (LL.M) from National Law University and Judicial Academy, Assam.

Date: 07/07/2022



Dr. Kailash Jeenger

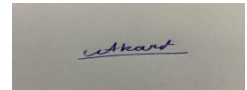
Associate Professor of Law

National Law University and Judicial Academy, Assam

DECLARATION

I Utkarsh Singh, do hereby declare that the dissertation titled “PERSONAL DATA PROTECTION AND INTERMEDIARY LIABILITY: A LEGAL STUDY” submitted by me for the award of the degree of MASTER OF LAWS/ ONE YEAR LL.M. DEGREE PROGRAMME of National Law University and Judicial Academy, Assam is a bonafide work and has not been submitted, either in part or full anywhere else for any purpose, academic or otherwise.

Date:7/7/2022



Utkarsh Singh

SM0221031

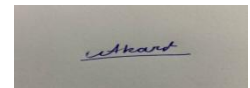
National Law University and Judicial Academy,
Guwahati, Assam

ACKNOWLEDGEMENT

I want to express my sincere gratitude to Dr. Kailash Jeenger (Associate Professor of Law), my guide for this dissertation at National Law University and Judicial Academy, Assam, for his able and constant guidance; without his advice and encouragement, the dissertation would not have been possible. He gave me clear insights into my project and valuable input at every step of this dissertation. I am highly obliged for his invaluable advice, directions and kind supervision.

I would also like to acknowledge the help provided by the IT Department and the Library Staff at National Law University and Judicial Academy, Assam; it was only through their support that I could access the required resources and complete my dissertation fruitfully.

I would also like to thank my peers who provided me with their valuable input and suggestions. Above all, I thank the National Law University and Judicial Academy, Assam. They provided me with the opportunity to pursue my interest in this given field, as a result of which I was able to work on this dissertation.



Utkarsh Singh

SM0221031

National Law University and Judicial Academy,
Guwahati, Assam

TABLE OF CASES

1. *Avnish Bajaj v. State*
2. *Amway India Enterprises Pvt. Ltd. and Ors. v. IMG Technologies Pvt. Ltd. and*
3. *Christian Louboutin SAS v. Nakul Bajaj and Ors,*
4. *Delfi v. Estonia*
5. *Dart v. Craigslist, Inc.*
6. *Google v. Visakha Industries,*
7. *Google v. Spain*
8. *Kent RO Systems Ltd. v. Amit Kotak*
9. *KS Puttaswamy v. Union of India*
10. *Kamlesh Vaswani v. Union of India*
11. *Magyar Tartalomszolgáltatók Egyesülete (“MTE”) and Index.hu Zrt (“Index”) v.
Hungary*
12. *Matthew Herrick v. Grindr LLC*
13. *My Space v. Super Cassettes Industries*
14. *Re: Prajwala*
15. *Sabu Mathew George v. Union of India*
16. *Shreya Singhal v. Union of India*
17. *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.*
18. *Viacom International v. YouTube.*

TABLE OF STATUTES

- 1950 - Constitution of India
- 1957- Copyright Act
- 1973- Code of Criminal Procedure
- 1986- Computer Fraud and Abuse Act
- 1994-Prenatal Diagnostic Techniques (Prohibition of Sex Selection) Act
- 1996- Communications Decency Act
- 1998- Digital Millenium Copyrights Act
- 2000- Information Technology Act
- 2000- European Union E-Commerce Directives
- 2000- Sarbanes Oxley Act
- 2000- Designs Act
- 2011- Information Technology (Intermediary Guidelines)
- 2011- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information)
- 2017- General Data Protection Regulation
- 2018- California Consumer Privacy Act

TABLE OF ABBREVIATIONS

1	Anr.	Another
2	v.	Versus
3	CrPC	Code of Criminal Procedure
4	CCPA	California Consumer Privacy Act,
5	CFAA	Computer Fraud and Abuse Act
6	EU	European Union
7	GDPR	General Data Protection Regulation
8	Govt.	Government
9	GNI	Global Network Initiative
10	HC	High Court
11	ICCPR	International Covenant on Civil and Political Rights
12	ICT	Information and Communication Technologies
13	ICO	Information Commissioner Office
14	IGF	Internet Governance Forum
15	IT	Information Technology
16	ISP	Internet Service Provider
17	OECD	Organization for Economic and Cultural Development
18	Ors.	Others
19	Pvt.	Private
20	SC	Supreme Court

21	SCIL	Super Cassettes Industries Limited
22	SMI	Social Media Intermediary
23	SSMI	Significant Social Media Intermediary
24	SOX	Sarbanes-Oxley Act
25	UDHR	Universal Declaration of Human Rights
26	UK	United Kingdom
27	UN	United Nations
28	UNGPBH	United Nations Guiding Principles on Business and Human Rights

TABLE OF CONTENT

SUPERVISOR CERTIFICATE.....	i
DECLARATION.....	ii
ACKNOWLEDGEMENT.....	iii
TABLE OF CASES.....	iv
TABLE OF STATUTES.....	v
TABLE OF ABBREVIATIONS.....	vi-vii
1. CHAPTER 1- INTRODUCTION.....	1-20
1.1. Introduction to Intermediary liability.....	1
1.2. Statement of Problem.....	7
1.3. Literature Review.....	8
1.4. Aim.....	16
1.5. Research Objectives.....	16
1.6. Scope and Limitations.....	17
1.7. Hypothesis.....	17
1.8. Research Questions.....	17
1.9. Research Methodology.....	18
1.10. Chapter Design.....	19
2. CHAPTER 2: THE ISSUE OF COPYRIGHT INFRINGEMENT AND BREACH OF PRIVACY BY INTERMEDIARIES.....	21-38

2.1. Definition of an Intermediary.....	21
2.2. Safe Harbor Provisions.....	25
2.3. Role of Intermediaries in Copyright Infringement.....	27
2.4. Breach of Privacy by Intermediaries.....	31
3. CHAPTER 3: INTERMEDIARY LIABILITY LAWS IN INDIA.....	39-56
3.1. Timeline of Indian Laws dealing with Intermediary Liability.....	39
3.1.1. Information Technology Act, 2000.....	41
3.1.2. Information Technology (Amendment) Act, 2008.....	44
3.1.3. Information Technology(Intermediary Guidelines) Rules, 2011.....	47
3.2. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.....	50
3.3. Complications brought in by the new rules.....	53
4. CHAPTER 4- JUDICIAL INTERPRETATION OF INTERMEDIARY LIABILITY.....	57-72
4.1. Avnish Bajaj v. State (2008).....	57
4.2. Shreya Singhal v. Union of India(2015).....	59
4.3. In Re: Prajwala (2015).....	60
4.4. Kamlesh Vaswani v. Union of India (2016).....	61
4.5. My Space v. Super Cassettes (2017).....	62
4.6. Kent RO Systems v. Amit Kotak (2017).....	65
4.7. Christian Louboutin SAS v. Nakul Bajaj (2018).....	67
4.8. 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 (2018).....	68
4.9. Sabu Mathew George v. Union of India (2018).....	69
4.10. Google India Pvt Ltd. V. Vishakha Industries Limited (2019).....	71

5. CHAPTER 5- INTERMEDIARY LIABILITY FRAMEWORKS	
 GLOBALLY	73-87
5.1. The European Union.....	74
5.1.1. Google v. Spain (2014).....	76
5.1.2. Delfi v. Estonia (2015).....	79
5.1.3. Magyar Tartalomzsolgaltatik Egyesulete (“MTE”) and Index.hu Zrt(“Index”) v. Hungary (2016).....	80
5.2. The United States of America.....	81
5.2.1. Dar v. Craigslist (2008).....	82
5.2.2. Viacom International Inc v. Youtube Inc. (2010).....	83
5.2.3. Matthew Herrick v. Grindr LLC (2019).....	84
5.3. International Doctrines relating to Intermediary Liability.....	85
6. CHAPTER 6- RECOMMENDATIONS AND CONCLUSION	88-100
6.1. Recommendations.....	88
6.2. Conclusion.....	92
 BIBLIOGRAPHY	 xi-xvi

CHAPTER 1-INTRODUCTION

1.1 Introduction to Intermediary liability

1.2 Statement of Problem

1.3 Literature Review

1.4 Aim

1.5 Research Objectives

1.6 Scope and Limitations

1.7 Hypothesis

1.8 Research Questions

1.9 Research Methods

1.10 Chapter Design

1.1 Introduction to Intermediary Liability

Today we cannot think of a world without the Internet; Internet has become an essential part of everyone's life. It has brought the world together and is presently used to perform various day-to-day tasks, be it the simple task of searching the meaning of a word to booking airplane tickets. It has now established an essential role in our lives, and most of our everyday activities now require Internet use. It has allowed people to bridge distances and interact with one another despite their location; social networking has increased extensively from Instagram to WhatsApp to Facebook. The services mentioned above may not have been possible without intermediaries who give the public a platform to perform these activities.

Intermediaries are online platforms that facilitate the transmission or exchange of information between two parties. Ideally, they are only to act as a neutral party throughout the transaction, and their role should be limited to that of a messenger. Initially, when the laws were being framed internet didn't exist; as a result, there were no laws that regulated these online platforms. Today's Intermediaries are handling not just standard data but also our sensitive personal data and personally identifiable information. Now the role of intermediaries as data repositories is becoming significant with each passing day. This data is collected not just over the internet but also through connected devices such as smartphone, smart televisions, watches etc. The year 2020-2021, due to the global covid pandemic, has already seen immense growth in the number of intermediaries springing up daily to provide various value-added services.

“Intermediary liability”, to put it simply, refers to the extent of liability that an intermediary stands to incur due to the non-permissibility under the 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 actual content creators. 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.

When the internet came about, intermediaries were considered to be bastions of free speech. Still, with time new complications came about and with the intermediaries, the laws governing intermediaries also evolved slowly. Initially, a blanket “safe harbor” was given to intermediaries against third parties so they could work freely without any intervention. Over time certain conditions were imposed on the intermediaries for availing of safe harbor protection; these conditions initially were only limited to self-regulation of illegal content on their respective platforms. With the protection under safe harbor provisions, these intermediaries saw unprecedented growth be it an online shopping app like Amazon, a video streaming service like youtube or a social media app

like Facebook. With the sudden growth of these platforms, the number of users that interacted with them also increased worldwide. For example, e.g. a Social Media Intermediary like Facebook gained millions of users in just three years; as a result, it became increasingly difficult for intermediaries to monitor illegal content on their respective platforms. With a lack of regulation, the problem of misuse of data began, misinformation became rampant, and users' privacy was severely threatened. These platforms, at various stages, also failed to assist law enforcement agencies; as a result, harassment and abuse of different vulnerable groups increased online.

There were no proper redressal mechanisms for such victims of abuse as the laws were not adequately implemented or were ambiguous in their wording. The intermediaries largely remained unregulated, and instead of rectifying the problem, they developed a new way to exploit its users further. The intermediaries started monitoring their users' browsing behavior to make revenue from advertising. Users' behavior while interacting with their platform was recorded and analyzed, and targeted advertisements were provided to users to influence their buying behavior. They also used this data to see the type of content their users liked and interacted more with so as to bombard their recommendations with similar content. This was done so that the users would spend more time on their platform. This way of doing business was in direct conflict with the intention of lawmakers that provided the intermediaries with safe harbor protection so that the intermediaries could freely work towards the benefit and growth of society. This was just one part of the problem; the lack of regulation led to a rapid spread of rumour and misinformation. In India itself, this spread of misinformation has led to the incident of lynching of over 65 people, generally done by a mob in the exercise of vigilante justice. These online rumours are spread rapidly through messaging platforms such as WhatsApp and often result in a massive hysteria, like in the case of Maharashtra Dhule district wherein a mob of over 3500 people gathered outside a government office to kill five labourers on suspicion of them being child-lifters.

Internet platforms have systematically failed to protect user rights in specific, 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 platform¹. In 2018, Facebook was used to spread Anti-Rohingya propaganda for inciting murders, rapes and the largest forced human migration in recent history. Most of Myanmar’s 18 million Internet users 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 broad reach of Facebook. The social media platform was accused of doing little to prevent harmful content from proliferating on its platform. Even though Facebook eventually deactivated the military personnel accounts, millions of sham accounts went undetected².

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. Senators Mark Warner and Amy Klobuchar introduced the Honest Ads Act following the use of Facebook advertisements by Russian provocateurs, which would require platforms to make “reasonable efforts” to bar foreign nationals from purchasing specific categories of political advertisements during the campaign³.

Intermediary liability, the focus of this dissertation, illustrates how the internet forced lawmakers to analyze and implement new approaches to an old legal construct, i.e. vicarious liability. Intermediaries like blogging platforms, discussion boards and social

¹ IndiaSpend, ‘Child-lifting rumours caused 69 mob attacks, 33 deaths in last 18 months’(Business Standard, 1 February 2017) < 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> accessed 17 April 2022

² Paul Mozur, ‘A Genocide Incited on Facebook, With Posts From Myanmar’s Military’ (New York Times, 15 October 2018) <<https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html> > accessed 17 April 2022

³ Andrew Mathew, ‘Russia ‘meddled in all big social media’ around US election’(BBC, 17 June 2019) <<https://www.bbc.com/news/technology-46590890> > accessed 9 May 2022

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 is specified under relevant laws and 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-harbor regime, and the Information Technology (Intermediaries Guidelines Rules), 2011 specified specific 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. Still, 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*⁴. Subsequently, on February 24, 2021, the Ministry of Electronics and Information Technology notified new Rules, thus amending 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".

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 imposing regulations on Internet companies must be mindful that such rules should not be over-broad, resulting in hampering fundamental digital rights such as privacy and free speech in the online world.

⁴ [2015] SC1532

The intermediary liability law in India is primarily governed by Section 79 of the IT Act, As per that provision, online intermediaries enjoy a safe harbor for third-party content on their platforms till they prescribe to specific due diligence rules set out under the Intermediaries Guidelines. Provisions under the Copyright Act, 1957 provide for some protection to certain intermediaries as well. Section 79 of the IT Act, in conjunction with the Supreme Court of India ruling in *Shreya Singhal*⁵, broadened the protection given to intermediaries and allowed them to take down content only on instructions by courts or authorised government agencies or the authoritative law of the land on intermediary liability. Though, it is pertinent 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 that infringes IP rights. 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.

This dissertation will briefly go over the current state of intermediary liability laws in the country, examine some notable litigations that have served to define the contours of this legal framework better. It will also highlight ongoing litigations that may significantly impact India’s intermediary liability regime in the future. It will 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 the right to privacy that is indirectly connected to intermediary liability but bear significant implications for it nonetheless. This dissertation does not claim to offer simple solutions to a complicated problem. It hopes to provide 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 inadequate regulations that facilitate censorship by proxy without addressing the notorious problem of “fake news”, breach of privacy and copyright infringement.

⁵ [2015] SC1532

1.2 Statement of Problem

Intermediaries are the online platforms that facilitate the transmission or exchange of information between two parties; technically, they are required to act as a neutral party throughout the transaction, and their role is that of a messenger between two parties. At the time of independence, when laws were being framed and adopted, these technological advances were not thought of; as a result, no laws regulated such platforms. Only through trial and error did laws governing intermediaries come into the picture on a global scale. India somewhere still lacks behind although it is steadily moving towards a positive direction to regulate such intermediaries”. In my research, I will be dealing with two critical issues faced by India when it comes to regulations governing intermediary liability, namely:

1. **Data protection and mismanagement:** currently, there are no concrete laws that dictate how these online platforms are to store the data of Indian citizens. There are also no strict laws that set out the consequence in case of a data breach; as a result, the data of citizens of India is readily available in the online space, and Indian citizens are left vulnerable in case of a data breach. The data collected is additionally used to monitor the browsing habits of the Indian citizens, and through this analysis, advertisements/posts are designed to influence the behavior of people online. With the introduction of the latest amendment, a new problem of privacy has also emerged as under the latest amendment. The government can ask any intermediary to provide them with the personal data of any citizen in specific scenarios. This paper will analyze these issues in depth by looking at the stance taken by Indian legislators and Judiciary and will also compare how countries like the USA and the EU tackle these issues.

2. **Copyright violation:** Intermediaries have time and time again been involved with copyright infringement suits, but due to the blanket protection being provided to intermediaries, they are rarely held liable for such breaches. This predicament leaves the authorities in a very peculiar position, for there is no clear-cut line as to when Intermediaries are to be held liable. Ministry of Electronics and Information Technology recently notified the Information Technology (Intermediary Guidelines and Digital Media

Ethics Code) Rules 2021 wherein some of these issues were dealt with, but these guidelines faced a massive backlash as there was no proper discourse in the parliament over these laws and the online platforms were asked to comply with the guidelines in a concise frame of time. Many other countries have introduced similar laws like European Union's GDPR and California's CCPA. In my research, I will compare the laws of such countries and how a country like India can take inspiration from such laws and make a proper framework to regulate Intermediaries and attribute appropriate liability in case of a breach. I will also analyse the stance the Indian Jurists, Lawmakers and the Indian Courts take to understand the reasoning behind the current laws.

1.3 Literature Review

The debate over Intermediary Liability is not limited to India; all key economies have recognized the role played by intermediaries in the online ecosystem and have made rules and regulations to govern both the privacy and intellectual property aspects it. This literature review seeks to synthesize the existing literature in relation to both of these aspects.

1. Law of Intermediaries, Pavan Duggal, 2016⁶

This book sheds light upon the latest existing position of the Indian Cyberlaw on the issue of intermediaries and their liability. This book further elaborates upon the distinct ways in which intermediaries can potentially limit their exposure to legal consequences and limit their liability. The author, through this book, has tried to uncover the emerging jurisprudential and legal position of intermediaries in India. The book is written in a layman's language and is very simple in its approach to answering the important question of what, according to the law, are intermediaries expected to do, what kind of protections they have under the Indian

⁶ Pavan Duggal, *Law of intermediaries* (1st edn, Universal Law Publication 2016)

law and what type of compliance requirements are mandated for intermediaries functioning in India.

2. Computers, Internet and New Technology laws, Karnika Sethi, Second Edition⁷

Author Karnika Sethi through this book, aptly highlights new laws, policies, cases, concepts, events and studies that have helped in the evolution of cyber laws in the national and international spheres, including new bills and guidelines. It especially focuses on the development of laws in India. The author of this book also talks about the problem of automating content removal and how that may affect “Free Speech” she further highlights the fact that even if automated moderators are allotted, they do not guarantee efficiency and accuracy as artificial intelligence is currently not mature enough to replace human judgment.

3. Law Relating to Computers Internet and E-commerce, Nandan Kamath, Fifth Edition, 2012⁸

The Author, through this book, deliberates upon the types of problems thrown up by the internet and the nature of gaps in the existing laws and practices. The author highlights the pitfalls in the current statutes and emphasizes the importance of appropriate cyber laws in India. The author, in Chapter 5 of his book, points to the mismatch in the application of Copyright Law and IT Act, while IT Act provides a safe harbor to the intermediaries who did not “actively participate” or had any knowledge of the transaction that led to the violation. On the other hand, the Copyright Act provides absolute immunity to the intermediaries as long as they had no reason to believe that the work was protected by copyright or that the storage of said work was only incidental. Finally, the author points to the role of

⁷ Karnika Sethi, *Computers, Internet and New Technology Laws*(2nd edn, Lexis Nexis 2016)

⁸ Nandan Kamath, *Computers Internet & E-commerce* (5th edn, Universal Law Publications 2014)

our lawmakers and courts in this internet-heavy world and how they have to actively review and revise cyber laws from time to time.

4. Computer Law, Chris Reed, Oxford University Press, 2013⁹

This book analyzes the unique legal problems that arise from computer technology and transactions carried out between users through the exchange of digital information. The topics covered in this book range from contractual matters, intellectual property protection, E-commerce, data protection and intermediary liability.

5. Cyber Law, Pavan Duggal, 2014¹⁰

This book is a comprehensive commentary, critique and analysis of various provisions of Indian Cyber Laws. This book not only examines all issues in the digital and mobile ecosystem that every user of the electronic format needs to keep in mind, but it also lays threadbare the existing challenge to the legal and regulatory frameworks that technology is posing and how there is a need for constant updating of cyber laws in India. The Author in chapter 12 has pointed out the ambiguities in the Intermediary laws. The author focused upon the “Active knowledge” aspect of intermediary liability and stated that ultimately the question of whether the intermediary was aware of the whole situation or not or whether their role in the whole transaction is only limited to that of an intermediary is to be decided by a court of law. The author also points out a difference between IT Laws and Copyright laws, wherein there is no obligation on an intermediary to restore content once removed, whereas under the Copyright act, the removed content needs to be restored.

⁹ Chris Reed, *Computert law* (2nd edn, Universal Law Publishing 2013)

¹⁰ Pavan Duggal, *Cyber Law* (1st edn, Universal Law Publication 2014)

6. Information Technology Law, Andrew Murray¹¹

This book discusses the law of the United States in relation to intermediary liability and Safe Harbor provisions. They discuss how the United States of America protects the Intermediaries from Copyright Liability through the Safe Harbor Provision of DMCA. This book sheds light on how intermediaries need to set up a proper notice and takedown mechanism. Once such a mechanism is put in place, then the intermediaries need to ensure that they act as neutral parties throughout the transaction and once that requirement is fulfilled, then they will be granted protection under the safe harbor provision of the DMCA. Although the umbrella under which the intermediaries are protected is huge, it creates the problem of people misusing the said notice and takedown provision for their own private benefit. Since the companies have no use in “not taking down” any content, they take down content from their website without much investigation to avoid any litigation or liability claims. This book profoundly indulges in the above mentioned aspect of safe harbor provisions.

7. Intermediary Liability 2.0 A shifting paradigm by SFLC¹²

This paper lays down a detailed analysis of the Intermediary liability framework in India and across different jurisdictions, namely the USA and Europe. The article profoundly analyses the cases across other jurisdictions and how each of these countries is dealing with different aspects of intermediary liability. The paper further elaborates upon the data protection aspect of Intermediary liability in the USA, and how each individual state has the power to make laws regarding the same, with one of the first enactments being the CCPA of California, the paper draws similarities between GDPR of European Union and CCPA and how Personal Data Protection Bill of India is still lacking behind. The paper highlights

¹¹ Andrew Murray, *Information Technology Law* (1st edn, Oxford University Press 2010)

¹² SFLC, ‘Intermediary Liability 2.0: A shifting paradigm’(2019) 1(1) SFLC <<https://sflc.in/intermediary-liability-20-shifting-paradigm>>

the international regulations regarding intermediary liabilities and how India and other jurisdictions have imbibed the same in their domestic laws.

8. Mondschein, C.F., Monda, C. The EU's General Data Protection Regulation (GDPR) in a Research Context.¹³

The authors in this paper have discussed the onset of GDPR in the European Union and how a positive example has been set for an active data protection law. They further highlight through the means of GDPR how law can be used to protect the private data of people and have also pointed out that since most of the companies have readily complied with the GDPR therefore if a country properly frames its set of rules regarding data protection, then the Data Protection aspect of intermediaries can be regulated.

9. 31st report of the “Parliamentary Committee on Subordinate Legislation”¹⁴

This report pointed toward the ambiguity present in the laws that deal with the question of intermediary liability. The lawmakers, through this report, pointed towards a number of ambiguities in regard to the Intermediary guidelines. The committee recommended that the ambiguous terms should be replaced with terms that are used globally, and their application has been tested. The committee, in its report, also recommended that there should be transparency and clarity in the notice and takedown procedure established in the guidelines so as to ensure that no parties suffer because of such ambiguity and to avoid abuse of the process. The government failed to incorporate any of the recommendations given by the committee.

¹³ Mondschein, C.F., Monda, C. *The EU's General Data Protection Regulation (GDPR) in a Research Context*, (Springer, Cham, 2018)

¹⁴ Law Commission, *Report of Parliamentary Committee on Subordinate Legislation*(Law Com 31, 2013)

10. Whastapp report on 2021 amendment¹⁵

Whatsapp, through this report, opposed the added provision of Traceability requirement brought in by the latest 2021 Rules; the new rules require the Intermediaries to allow tracing of the originator of particular information as and when required by the government. This requirement not only affects the right to privacy which is enshrined in the fundamental rights¹⁶, the same of which was affirmed in the KS Puttaswamy vs UOI¹⁷ judgment but also affected the end-to-end encryption model followed by WhatsApp, which guarantees that a third party cannot decode personal messages between users. Breaking such encryption will also result in a blatant breach of privacy, as stated by the report on their end-to-end encryption model. The recent amendment makes it mandatory for the SSMI to set in place an automated system that actively filters content being uploaded by users, the SSMI is required to play a neutral role and are to only serve as a medium. Still, the point of contention here is that if the task of filtering and blocking content is given to intermediaries, then they will have the task that is undertaken by the judiciary as it is nowhere stated in the provisions as to what is to be considered “unlawful”. This concept of filtering content goes against the judgment set down in the Shreya Singhal case¹⁸. Since no active way of filtering content is laid down therefore, intermediaries will take down all content which is reported in order to avoid liability, such takedown of content will result in the form of private censorship. Whatsapp through this report pointed out the flaws in the new amendment and requested the Indian lawmakers to rethink about implementing the same.

¹⁵ Whatsapp Report, ‘Intermediary Liability & Freedom of Expression’(Whatsapp 17 March 2021)<<http://cis-india.org/internetgovernance/intermediary-liability-and-foe-executive-summary.pdf>> accessed 3 June 2022

¹⁶ The Constitution of India(1950) art21

¹⁷[2017] SCC 1

¹⁸[2015] SC1532

11. The Online Intermediary Liability Research Project, University of Washington School of Law, Center for Advanced Studies and Research on Innovation Policy, 2018¹⁹

This Project generated research papers from multiple countries on intermediary liability issues for online service providers in the following topic areas: Defamation, Child Protection, Hate Speech, and Privacy. The authors in the said research papers have extensively studied the issue of data privacy and the spread of misinformation in India.

12. Internet Intermediary Liability: Wilmap, Theory And Trends, Giancarlo F. Frosio, The WILMap Project²⁰

The WILMap is a graphic interface for laws and court decisions that enables the public to understand intermediary liability regimes worldwide and how changing Internet laws affect user rights and freedom of speech. Visitors can choose information on specific countries of interest, including case law, statutes, and proposed laws, from this comprehensive English-language resource. Links to the original sources and, if available, English translations are provided on each nation page. According to the WILMap website, this tool aims to "learn about intermediary liability regimes worldwide and to identify regions where legal regimes balance—or fail to balance regulatory goals with free expression and other civil freedoms." The WILMap lists laws, ongoing legislation, and initiatives that would impose requirements on intermediaries, including hosting and access providers as well as other internet intermediates as payment processors. The WILMap addresses a wide range of issues, including but not limited to the safe

¹⁹University of Washington, 'The Intermediary Liability Project' (2017) UOW <<https://www.law.uw.edu/programs/liabilityresearch/country-reports>>

²⁰ Giancarlo F. Frosio, 'Internet Intermediary Liability: WILMAP, Theory and Trends'(2017) 13(1) IJLT <<https://www.ijlt.in/journal/internet-intermediary-liability%3A-wilmap%2C-theory-and-trends>>

harbors for online intermediaries, e-commerce, copyright and trademark protection, defamation, hate speech and other problematic speeches, including anti-terrorism provisions, privacy protection, and online child safety.

13. Implementing the EU Copyright Directive by FIPR²¹

The authors at fipr in this paper have discussed the Copyright protection laws in the European Union. Regarding copyright protection, the authors highlight that the EU has clearly shown its stance through the various judgement given in prospect of copyright protection. The author stated that through a study of cases the court's stance could be interpreted as "one could not expect the intermediaries to regulate and check each and every piece of information stored on their website". The authors studied the judicial intent behind this decision and concluded that the reasoning behind this judgment was to protect the "right to impart information on the internet" in the European Union. This paper circles around the regulation of content by intermediaries and sheds some light on how stricter regulations could lead to a restriction on freedom of speech and expression.

²¹ FIPR, 'Implementing the EU Copyright Directive' (FIPR, 12 June 2011)
< <https://www.fipr.org/copyright/guide/eucd-guide.pdf>>

1.4 Aim

This research aims to analyze the intermediary laws in India with reference to Data Protection and Intellectual Property Infringement. This dissertation focuses on the functioning of Intermediary laws across the USA and EU to determine whether India's current intermediary liability laws are efficient in dealing with the emerging issues of data privacy and protection of an individual's IP rights. This research finally tries to find a possible solution to improve India's current intermediary liability ecosystem.

1.5 Research Objectives

1. To understand the concept of Intermediary liability and its functions in the present time.
2. To analyze the current Intermediary liability ecosystem in India.
3. To study the safe harbor provisions concerning intermediary liability
4. To trace the view of the Indian courts and their interpretation of the laws relating to intermediary liability.
5. To examine the different approaches countries take in dealing with issues relating to Intermediary liability management.
6. To find out the most effective and practical method to balance intermediary liability and safe harbor provisions for a country like India.

1.6 Scope and Limitations

The research explores and formulates the Indian legislator's and courts' approach to determining the liability of an intermediary in India. These decisions are widely scattered in innumerable judgments and across various laws passed in different circumstances. The research further explores the laws and judicial pronouncements in USA and Europe as well as principles set forth by international law. This research seeks to understand the problems in India's current Intermediary liability framework.

The scope is limited to the decisions passed by the judiciary, laws laid down by the parliament of India, judicial pronouncements of the courts of USA and EU. Intermediary liability is a topic that spans across each and every jurisdiction across the world, but herein the study is confined to mainly India USA and EU. It is further constrained by time, and because of the niche nature of the topic, the research is done using readily available books and online research material

1.7 Hypothesis

India's present intermediary liability framework is inadequate for solving emerging problems.

1.8 Research Questions

1. Whether the current statutes dealing with intermediary liability can tackle the problems brought on by the current digital age?
2. Whether blanket safe harbor provisions are practical in the present day and age?
3. Whether there is a need for a new intermediary liability ecosystem in India?

1.9 Research Methodology

The research methodology to be followed for this research study would be the doctrinal research method. The study will analyze in detail the scope and provisions of the existing laws and their effect and consequences. The study will also examine the current laws of the European Union and The United States of America.

The study will analyze the judgements delivered by courts in India and that of the EU and the USA. The study will examine the Data collected from primary and secondary sources, including but not limited to opinions of lawmakers, government websites, Judgements given by Indian courts, international courts, and books/published research papers written by experts on the relevant topic.

1.10 Chapter Design

Chapter 1: Introduction

This chapter will introduce the topic of this dissertation, i.e. Personal Data Protection and Intermediary Liability: A Legal Study. It will lay out the statement of the problem of this research as well as the aims and objectives that this research seeks to fulfil. This chapter will elaborate upon the hypothesis and the research questions that will be answered in the subsequent chapters and will explain the methodology that will be used to answer these questions. Finally, this chapter will review the literature that helped in answering the questions raised in this dissertation.

Chapter 2: The issue of Copyright Infringement and Privacy Breach by Intermediaries.

This chapter will give a brief background of how the Intermediary liability ecosystem works in India and will further explain the key factors and challenges like the safe harbor provision, copyright infringement and Breach of privacy that the current Intermediary Liability ecosystem in India faces at the present times.

Chapter 3: Intermediary Liability Laws in India

This chapter will shed light on India's development and growth of Intermediary laws. It will discuss the parliamentary intent behind these legislations and the changes brought on by each amendment. Finally, it will discuss the latest amendment of 2021 and the challenges it brought.

Chapter 4: Judicial Interpretation of Intermediary Liability in India

This chapter will analyze the critical judgments made by the Indian Courts to peruse their view on the issue at hand.

Chapter 5: Intermediary Liability Frameworks Globally

This chapter will analyze the Intermediary Liability frameworks of global economies like the USA and European Union to understand their approach to tackling Intermediary related problems. Finally, it will examine the frameworks and guidelines set forth by the International Institutions in relation to the handling of Intermediaries.

Chapter 6: Conclusion and Suggestions

This chapter will sum up the findings that can be observed from this dissertation and discuss the research questions' results. It will also try to give suggestions on how intermediary liability should be dealt with in India.

CHAPTER 2: THE ISSUE OF COPYRIGHT INFRINGEMENT AND BREACH OF PRIVACY BY INTERMEDIARIES

2.1 Definition of an Intermediary

2.2 Safe Harbor Provisions

2.3 Role of Intermediaries in Copyright Infringement

2.4 Breach of Privacy by Intermediaries

2.1 Definition of an Intermediary

In the context of the internet, an Intermediary is an entity that, through its platform, facilitates the flow/exchange of data all over the internet. The moment a person connects to a network to access the internet, they automatically start dealing with several intermediaries. Functions performed by an intermediary are diverse and are not strictly limited to a single field. They are huge data repositories who have managed, processed, dealt and handled vast volumes of data; ever since the data explosion brought on by 4G technology, more and more intermediaries are coming up to provide a wide array of data-driven services. Intermediaries today deal with not just average data but also the personal data of their users; this data also includes personally identifiable information. These enterprises are generally run by private entities that provide services and platforms to facilitate the online exchange of information or transactions between two parties. There is no clear-cut distinction between types of intermediaries, but they can be broadly categorized into two, i.e. (1) A Telecom Service Provider (TSP) that provides the service of supplying and setting up network-related infrastructure for, e.g. Providing Optic Cables for internet connectivity or providing spectrum bandwidth through which data is transferred on the internet. ISPs are a form of TSP that offer web connectivity to the public. (2) Service Providers provide a myriad of services for the end-users to leverage the real power of the internet to enable efficient management of activities such as

education, entertainment and social networking. The OECD proposed that “Internet intermediaries” be defined as follows²²:

“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.”

In India, The Information Technology Act, 2000 governs the actions of intermediaries and Section 2(1)(w)²³ of the Act prior to the amendment broadly defined the term intermediary as: “any person who on behalf of another person receives, stores or transmits that record or provides any service concerning that record; this 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” Therefore any entity that provides a platform for the exchange of goods/information between two parties such an entity would come under the broad spectrum given under Section 2(1)(w)²⁴ of the Information Technology Act, 2000.

The definition stated under the Indian law is comprehensive and non-exhaustive; it covers every entity indulging in the act of receiving, storing or transmitting electronic records; therefore, all kinds of websites, namely- blogging platforms, message boards, e-commerce websites, are covered under it. From the definition above, it can be said that the principle of intermediary liability is somewhat based on the principle of vicarious liability, i.e. just like the “principal is liable for the actions of the agent in case of vicarious liability”, in this case, the service provider is liable/accountable for any illegal act of a user on their platform. To ensure that such problems do not occur, the intermediaries need to regulate data flowing through their platform, but, due to the mass number of users and the humongous size of the data, it becomes nearly impossible to

²²OECD, *The Economic And Social Role Of Intermediaries* 2010.

²³ Information Technology Act(2000) s.2

²⁴ ibid

peruse all this data and ensure that no legal breach occurs. Therefore countries have come up with various “Intermediary Liability” laws and guidelines that state in what cases are intermediaries to be held liable and in what cases can they claim the protection of the law²⁵.

Intermediaries need to remain neutral throughout an active transaction, be it the upload of a piece of information or be it an exchange of messages between users. The term Intermediary liability generally comes into the picture when an intermediary somehow becomes a participant in a transaction; it refers to the liability that will be attributed to an intermediary in case he participates in an online transaction or if any form of unlawful content is found on their website. The authorities first check if the intermediaries were actively involved in the transaction and if they are found to be active participants, then they are held liable for the breach on their part. If it is found that the intermediary was not in any way involved in the transaction, then in such a case, they will not be held strictly liable for the infringing content on their platform. Users of the platform are posting content; therefore, the predominant consensus is that the said users should be held liable for the infringing content and not the platform. This is also what the laws in India agree with but in countries like China and Thailand the platforms are held strictly liable for the content available on their platform; in these countries, it is the absolute duty of intermediaries to ensure that the content posted by the users of their website is in line with the laws of the country²⁶.

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*”²⁷. These are:

²⁵ Duggal (n 6) 153.

²⁶ SFLC, ‘Intermediary Liability 2.0: A shifting paradigm’(2019) 1(1) SFLC <<https://sflc.in/intermediary-liability-20-shifting-paradigm>> accessed on 11 May 2022

²⁷ Article 19, ‘Internet Intermediaries: Dilemma Of Liability’(2013) <https://www.article19.org/data/files/Intermediaries_ENGLISH.pdf> accessed on 11 May 2022

1. **The Strict Liability Model:** User-generated content is subject to absolute liability for intermediaries. To comply with the legislation, intermediaries must monitor material; otherwise, they risk several penalties, including the revocation of their business license and/or criminal charges. China and Thailand are two examples.

2. **The Safe Harbor Model:** If intermediaries adhere to specific legal standards, they are granted conditional exemption from liability stemming from user-generated content. This model is further broken down into:

The vertical model: Liability is established in accordance with the nature of the in-question content. There are no differences made between the types of services that intermediaries offer, such as hosting vs transmitting.

The horizontal model: Liability is determined by the type of function the intermediary performs. Thus, intermediaries functioning solely as content transmitters may be completely protected from liability, whereas intermediaries acting as hosts may be subject to stricter regulations. If the latter do not promptly remove illegal content after being told, they risk losing their immunity. The "notice-and-removal" processes, legally required procedures that specify how content takedown requests must be received and handled by intermediaries, are another characteristic of the safe-harbor paradigm. To further stop the publication of illegal content, intermediaries may be urged to implement technology-based or self-regulatory content filters. The EU e-commerce Directive²⁸, US Digital Millennium Copyright Act and the Indian IT Act are legislations that employ this model of intermediary regulation.

3. **The Broad Immunity Model:** Broad, occasionally conditional exemption from liability resulting from user-generated content is granted to intermediaries.

²⁸ 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 OJ L 97/21

Notably, intermediaries are explicitly released from any responsibility to check for illegal information. Instead of viewing intermediaries as content publishers, this model views them as messengers who only transfer content on behalf of users. The Communications Decency Act²⁹ serves as an illustration of this design.

2.2 Safe Harbor Provision

In this era of the internet, people around the globe share information on social media and rely on it for entertainment etc. The internet gives everyone a right to put forth their views online for everyone to read; this information posted by a user may not always be accurate. In some instances, such platforms are deliberately used to spread misinformation and create unrest among citizens of a country; in such cases, an intermediary should not be held responsible if his only purpose was that of providing the user with a platform and he was not involved in the regulation of such infringing content online. In such cases, the safe harbor provision comes into the picture, a safe harbor is a provision within a statute that clearly specifies that in certain cases, an otherwise infringing act will not be deemed to violate a said rule. The Safe Harbor provision protects the intermediary from the actions of third parties as long as certain conditions are met, this provision acts as a shield and protects the intermediaries from any legal liability attributed to them because of the act of third parties.

Section 79 of the IT Act, 2000 talks about safe harbor provisions relating to intermediary liability in India; this section protects the intermediaries from being sued for infringing content/data uploaded on their platform by a third party of which they have no knowledge or control, provided they comply with the “due diligence” requirements outlined in the given provision. The intermediary must first and foremost ensure that its operation's scope is restricted to granting access to the electronic medium. They are not legally required to own any exclusive rights to the aforementioned electronic medium. The law

²⁹ Communications Decency Act(1997) s.230

does not mention the numerous licensing requirements in this context, and it is likewise unconcerned with how the intermediary provides access to the electronic medium. The primary responsibility of the intermediary must be to grant third parties access to an electronic medium where information is sent, temporarily stored, or housed. The second mandatory condition is that the intermediaries need to ensure that they were not involved with (i) Starting the said transaction, (ii) Choosing the receiver of the said transaction and (iii) Making changes to the information contained in the transaction. Therefore this provision protects the intermediaries from all forms of liability provided that the said data was being broadcasted without their knowledge and the intermediaries had adhered to the “due diligence” requirements.

In the case of *Christian Louboutin SAS v. Nakul Bajaj and Ors*³⁰, the Delhi High Court made a distinction between "active" and "passive" intermediaries when determining the responsibility of the e-commerce site darveys.com in the context of an alleged violation of the trademark rights of Christian Louboutin, whose products were being sold on the said platform. The Single Judge Bench held that “determination of whether an e-commerce platform is entitled to safe harbor protection under the IT Act³¹ will depend on whether it plays an ‘active’ or a ‘passive’ role while operating such a platform. The court identified a list of factors, including identification of the seller and providing details of the seller; providing quality assurance, authenticity guarantees or storage facilities; assistance for placing a booking of the product (including call centre assistance); creating a listing of the product; packaging of the product with its own packing; transportation, delivery, and advertising products on the platform, etc., involvement of such kind that would make the e-commerce entity an active participant” and observed that “*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*”. It further held that,

³⁰ [2018] DLT728

³¹ Information Technology Act(2000) s.79(1)

“any active contribution by the platform or online marketplace completely removes the ring of protection or exemption which exists for intermediaries under the IT Act.³²”

When addressing the question of whether the provision of incidental services by Amazon, Cloudtail, and Snapdeal, such as warehousing, packaging, storage, entering into new warranties, etc., could deprive them of the protection under Section 79, the Delhi High Court's Division Bench in the case of Amazon Seller Services Pvt Ltd v. Amway India Enterprises Pvt. Ltd³³. and Ors pointed out that Section 79 does not make a distinction between active and passive intermediaries. It was observed by the Division Bench that *“restricting the protection under Section 79(1) to ‘passive intermediaries’ would be a misinterpretation of Section 79”*. It further observed that *“there is prima facie merit in the contention of the Appellants that the value-added services provided by them as online marketplaces as listed out by the Single Judge, do not dilute the safe harbor granted to them under Section 79”*. The concept of classifying intermediaries as active or passive participants to establish the availability of safe harbor protection was effectively abandoned in the Amazon Case. However, the Division Bench refrained from discussing the claim's merits, saying that this would be tested and decided in a trial.

Thus, it must be determined whether an intermediary satisfies the requirements outlined in Sections 79(2) and 79(3) of the IT Act to claim exemption from liability under Section 79(1).

2.3 Role of Intermediaries in Copyright Infringement

The problem of who is to be held liable in cases of copyright infringement on an online platform has been discussed since the internet and remains a cause of contention to this day. Such infringement can occur if the intermediary is found to be in violation of the said copyright or his platform was used, and he was an active participant in the said

³² Information Technology Act(2000) s79

³³[2019] SC 397

transaction. This issue of Copyright infringement is broad in nature as it is not strictly limited to one country but expands internationally as the internet has no boundaries and content once uploaded on a public platform can be accessed by anyone from anywhere in the world. Under the Indian laws, The laws protecting copyright³⁴ , when read together with the Intermediary liability provisions of the Information Technology Act, 2000, provides a blanket safe harbor provision to protect intermediaries from liability of 3rd parties provided that the intermediary follows the given takedown and observation procedures and has followed the due diligence requirements set forth.

Section 81 of the IT Act provides that: *“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 or the Patents Act, 1970”*.

The proviso to this clause forbids the use of the IT Act's provisions to prohibit a person from exercising legal rights granted by the copyright or patent laws. The case of My Space v. Super Cassettes Industries Ltd³⁵ addressed the impact of this proviso on the responsibility of an intermediary under Section 79 of the IT act. The court ruled in the aforementioned case that Section 79 of the IT Act is intended for all other internet offences where intermediaries may be involved, including but not limited to auctioning, networking, servicing, news dissemination, and uploading of pornographic content, but not necessarily related to copyright infringement or patent infringement because those offences have been expressly excluded by way of Section 81 of the IT Act, 2000³⁶. But this judgement also helped in establishing the actual knowledge requirement, in regards to the same the court held that *“57... If copyright owners, such as SCIL inform Myspace specifically about infringing works and despite such notice it does not take down the*

³⁴ Copyright Act(1957)

³⁵[2017] DLT 478

³⁶SFLC, ‘Intermediary Liability 2.0: A shifting paradigm’(2019) SFLC <<https://sflc.in/intermediary-liability-20-shifting-paradigm>> accessed 11 May 2022

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 the notice.”

In India, a company that acts as an intermediary and allows users to share and circulate video files, music files, and films is liable under Section 51 of the Copyright Act, 1957, which states that any action that infringes on the author's or copyright holder's exclusive rights constitutes copyright infringement. A copyright owner's sole right under Section 14 of the Copyright Act of 195 is to make copies of any work using any medium and to communicate it to the public. Thus, a website like Napster or a network similar to it operating in India would be guilty of the crime of copyright infringement. Even if it is argued that the said intermediary is merely providing an indexing or listing service and not really transferring any files, Section 63 of the Copyright Act of 1957 will still be in effect. It states that anyone who "knowingly infringes" or aids the infringement of copyright in a work or other rights granted by the act, excluding the right under Section 53A, shall be punished with imprisonment for a term not less than 6 months but may extend to three years and a fine of not less than Rs. 50,000 but may extend to Rs. 2 lakhs. After the coming of 2011 rules³⁷, Intermediaries are now also required to inform their users to not publish any such content on their platform that “infringes any patent, trademark, copyright or other proprietary rights”. There is some relief for the intermediaries from copyright infringement, but such protection is conditional and limited to only certain instances. Section 52(b) and (c) of the Copyright Act provides protection to intermediaries 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

³⁷ Information Technology (Intermediary Guidelines), 2011

reasonable grounds for believing that such storage is of an infringing copy (actual knowledge requirement) ”.

The notice and takedown method in Section 52(c) allows copyright owners to ask intermediaries to remove protected content from their platforms for at least 21 days (or for a more extended period in case of a court order mandating such requirement). This clause mandates that intermediaries remove content after being satisfied within 36 hours of being intimate. Therefore a conjoint reading of the Copyright Act and IT Act would show that intermediaries need to conform to a higher standard of diligence regarding copyright-protected content. They must ensure that infringing content is not uploaded on their platform for everyone to see. The My space judgement also clarified that intermediaries are not required to immediately take down content on any form of unspecified notice as such takedowns will violate the right to free speech³⁸. Keeping in mind the actual knowledge criteria laid down in the MySpace case, the following inferences can be made

- a) Courts have distinguished the “actual knowledge” requirement for matters of free speech from claims of IP infringement. Courts have operationalized the notice-and-takedown system in IP proceedings, allowing right holders to ask that intermediaries remove infringing content after notifying them of the violation (the notice and takedown mechanism).
- b) Such demands must be specific and not overly general; rights owners may not ask intermediaries to be on the lookout for any potential infractions as this would necessitate ongoing monitoring and screening, which is not the function of intermediaries (the specific knowledge requirement).

³⁸ Mukul Sharma, ‘Safe Harbor Protection for E commerce platforms’ (CAM, 15 February 2021) <<https://corporate.cyrilamarchandblogs.com/2021/07/safe-harbor-protection-for-e-commerce-platforms/>> accessed 9 May 2022

Although courts have acknowledged that intermediaries cannot and should not act as judges in determining what content is unlawful or legal, they have also made it more challenging for intermediaries to defend instances of fair use or fair dealing by giving rights owners the authority to send notices for the removal of specific content³⁹.

2.4 Breach of Privacy by Intermediaries

Today, the right to privacy is regarded as a fundamental human right, and various international treaties and agreements impose duties on states to respect citizens' right to privacy. One such document is the Universal Declaration of Human Rights⁴⁰, the first comprehensive agreement between countries with a particular focus on the rights and freedoms of all human beings. It was adopted by the United Nations (UN) in 1948. India supported Article 12 of the UDHR, which guarantees the right to privacy by stating that a person has the right to legal protection from any arbitrary intrusion. In 1979, India ratified the International Covenant on Civil and Political Rights. Article 17 of the ICCPR states that “no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home, correspondence, nor to unlawful attacks on his honour and reputation” and that “everyone has the right to protection of the law against such interference or attacks”

Data has taken on enormous relevance in the digital age as the medium of exchange for the online economy. The fact that most well-known social media platforms, like Twitter and Facebook, do not charge users for their services and instead generate significant revenue from selling user demographic information to advertisers demonstrates the versatility and worth of data. Due to the disparity in power between data processors (both public and private) and individual users, this "information market" can substantially

³⁹ 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) <<https://spicyip.com/2019/02/saregama-pa-rdon-me-you-have-the-wrong-address-on-the-perils-and-pitfalls-of-notice-and-takedown.html> > accessed 19 May 2022

⁴⁰ UDHR(1948)

violate an individual's right to privacy. In this new paradigm, it is in the best interest of both private businesses and civil society to establish open legislative frameworks and encourage users of the internet to put their trust in them. The right of an individual to successfully control the information that relates to them is what constitutes privacy and not the complete absence of information about that person in the public domain. In other words, the right to privacy includes the individual's ability to exercise self-determination or the ability to manage their online identity⁴¹. This right has two components:

1. Other people and organizations shouldn't be given access to someone else's personal information without their consent.
2. A person must have significant control over the information they submit and how it is used.

This underlines the requirement for regulation of all data collection and uses elements, including the types of data that may be gathered, the sources from which they may be obtained, the purposes for which they may be employed, and the security precautions that those collecting such data must take. A developing economy like India, which has established its footing in the global economy by dominating the market for outsourcing and processing data from businesses all over the world, and is attempting to position itself as an appealing location for businesses, must develop strong and enforceable data protection standards⁴².

The internet is a unique medium for information exchange that holds a tonne of data made up of information that is saved, uploaded, downloaded, linked, or distributed via computers, mobile phones, and other devices. As more and more people use the internet to browse and post personal information online, especially on social networking platforms, the public now has easy access to information about parentage, educational background, interests, and even private photos and videos. Almost no confidential

⁴¹ Kamath (n 8) 172

⁴² University of Washington, 'The Intermediary Liability Project' (2017) UOW <<https://www.law.uw.edu/programs/liabilityresearch/country-reports>> accessed 7 May 2022

information remains safe from the confines of this virtual world. Data thefts, business espionage, identity theft, and other crimes, such as kidnapping, slander, and even murder in some extreme circumstances, have become widespread occurrences. Cybercriminals frequently utilise the internet to break into secure systems that contain vital data for a nation's defence. Credit rating companies, payment processors, staff members, income tax offices, service providers, and individuals collect sensitive personal data online. According to a number of recent press reports, data is maintained in an unencrypted format and is accessible to anyone who can gain access to the said device. When registering or setting up a new account to use a website's services, a user is frequently prompted for personal information. For instance, advertising organisations set up cookies to research online users' preferences and interests; they use this information to broadcast products on the users' system, which through the retention of the information they can now predict; this strategy used by websites is known as "behavioral advertising". Before obtaining the consent of the person whose private information is being sold, advertising companies frequently sell the data they acquire to third parties for profit. On the internet, a new practice known as "history sniffing" is on the rise, in which web browsers interact with websites and keep track of a website that the user has visited⁴³.

To maintain and safeguard the privacy and confidentiality of data and information, Section 72 creates a new offence. It states that anyone who has obtained access to any electronic record, book, register, correspondence, information, document, or other material in accordance with any of the powers given to them under the Information Technology Act of 2000, Rules and regulations made thereunder, is obligated to keep it a secret from others. Suppose the information is shared without the approval of the individual in question. In that case, the intermediary will be liable under Section 72 of the Act and will be subject to a fine up to one lakh rupees, or with imprisonment of up to two years or both.

⁴³ SFLC, 'Intermediary Liability 2.0: A shifting paradigm'(2019) SFLC <<https://sflc.in/intermediary-liability-20-shifting-paradigm>> accessed 11 May 2022

The Information Technology Act of 2000 grants the power to the Certifying Authorities, Adjudicating Officers, Deputy Controller of Certifying Authorities, Assistant Controller, or any other officer designated under the Act. Any of the individuals mentioned above are subject to punishment under this section if they obtain access to an electronic book, register, correspondence, information, document, or other material while acting under the authority granted to them by the Information Technology Act of 2000, Rules and regulations made there under, and disclose it to another individual without the consent of the owner of the data then the individual in question will be liable for punishment under the given section⁴⁴.

The present section⁴⁵ aims to ensure the confidentiality of data or information belonging to different persons. However, the scope of the section is limited to breach of confidentiality of information or data by relevant statutory authorities, which have secured access to the same in pursuance of their statutory powers. The section does not target the commonly prevalent breaches of confidentiality committed by lay netizens and users. It is pertinent to mention that the entire Information Technology Act, 2000 is silent on the contentious privacy issue, barring sections 72 and section 66E. The word “privacy” does not find mentioned in the body of Section 72 but is only mentioned in its heading.

Man actively interacts with society at large, and this interaction is essential for his day-to-day functioning. Still, he values his private space, a limited region that is inside the boundaries of his exclusive territory. In the actual world, we are all accustomed to the idea of internet privacy. Special laws protecting people's privacy are present in several nations nowadays. When the internet initially emerged as a medium, it sparked a heated discussion. Whether privacy is possible for users of the internet? After a great debate, it was agreed upon by all parties that each person has the right to preserve his or her own internet privacy. The second issue that arose was how to safeguard people's internet

⁴⁴ Information Technology Act(2000) s72

⁴⁵ ibid

privacy. On this complex cyberlaw problem, different governments have had divergent views. One of the most divisive legal concerns appearing in cyberspace is privacy. Privacy is critical to not only individual netizens but also businesses and governments, just like in the real world.

The privacy of online users has become very important at this time. Regarding the Indian situation, our nation lacks a comprehensive privacy law. We don't even have a privacy statute like some other nations have. The judiciary has been given the authority to interpret privacy in light of current laws. The Supreme Court of India has ruled that the right to privacy is a crucial component of the fundamental right to life that is found under Article 21 of the Indian Constitution. In *People's Union for Civil Liberties (PUCL) v. Union of India*⁴⁶, the Supreme Court has held: *Right to privacy is a part of the right to life and personal liberty enshrined under article 21 of the Constitution. Once the facts in a given case constitute a right to privacy, article 21 is attracted.*" The Parliament passed the Information Technology Act of 2000, India's first cyberlaw without addressing the critical problem of privacy. There is no definition of privacy under the Information Technology Act of 2000. The crucial issue of online privacy protection is not even mentioned anywhere under the Information Technology Act, 2000. Only the title of section 72 mentions privacy. Reading section 72 of the Information Technology Act, 2000 reveals that it was written in a restrictive manner and punishment is accorded to only those people who disclose any electronic record, book, register, correspondence, information, document, or other material to anyone after gaining access to it without the owner's consent⁴⁷.

Regarding the invasion of a person's online privacy, it is irrelevant. The Information Technology Act of 2000 makes no mention of spamming, or the practice of sending unsolicited emails to various recipients. The reality is that every time a netizen receives an unsolicited email, that in and of itself is a breach of that person's privacy. Because of

⁴⁶ [1997] SCC 301

⁴⁷ Duggal (n 6) 117

this, many US states, including Nevada, have passed laws prohibiting sending of spam emails online. Additionally, many websites currently collect user information that is frequently not protected and is sold to other businesses for financial gain. In other instances, hackers get access to the servers of websites that contain sensitive consumer information and steal the data for financial gain. The stolen data is then invariably sold to various businesses, which send unsolicited emails to multiple people's email addresses. These numerous endeavours all constitute a severe invasion of privacy⁴⁸.

In addition to the sections previously mentioned, Section 69 of the IT Act, 2000 grants the Central Government or the State Government the authority to issue directives for the “interception, monitoring, or decryption of any information through any computer resource to protect India's sovereignty, defence, security, and relations with friendly foreign states, as well as to uphold public order, prevent incitement to commit any cognizable offence, or for investigative purposes”. The subscriber or intermediary is required to give the intercepting agency all assistance in order to secure access to a computer that is generating, transmitting, receiving, or storing such information, as well as to intercept, monitor, or decrypt the data, or to provide information stored in computer resources. The Central Government is given the authority to make directives for prohibiting public access to any information via a computer resource under Section 69A. Similarly, Section 69B⁴⁹ gives the Central Government the power to track and gather data about internet traffic using any computer.

The party that owns the information will be harmed by an unlawful disclosure or use of the disclosed information by a person authorized to carry out conferred responsibilities, which is why Section 72 of the law provides a remedy when a private contractor commits such a violation. Penalties for confidentiality breaches are prescribed by Section 72A of the IT Act, 2000. Affected individuals may file a claim for damages before the adjudicating authority designated by Section 46 of the IT Act, 2000. The same action is

⁴⁸ University of Washington, ‘The Intermediary Liability Project’ (2017) 1(1)UOW <<https://www.law.uw.edu/programs/liabilityresearch/country-reports>> accessed 7 May 2022

⁴⁹ Information Technology Act 2000, s 69(A-B)

possible even if a corporate body disregards the IT Act, 2000, which requires that appropriate security methods be adopted to protect persons' personal data.

Unfortunately, India has relatively low levels of understanding about privacy in the real world and online. It is crucial that the government pass laws governing online privacy. Websites must be required to abide by tight rules regarding a variety of matters relating to personal privacy. Websites are required to inform users what information is being collected about them, what information is being collected about them, why it is being gathered, and how it will be used⁵⁰. Additionally, internet users should have the option to decide whether the data collected about them will be utilised for anything other than completing the transaction for which it is intended. In any such scenario, one should have the option to choose whether that website should utilize the information they provide about themselves to a website for purchasing music for any other reason than to carry out the transaction of selling music to the said individual.

Additionally, netizens should have access to good facilities under cyberlaw. Once a person provides information about himself to a website, they must be able to see that information, have a reasonable opportunity to correct any errors or update it, and the option to delete all of the data or information the website has acquired about them. Additionally, it is crucial for all websites, portals, and businesses to make sure that the user data they receive is treated carefully to prevent theft or unauthorized access. Self-regulation is a topic that the online industry has long disputed. Self-regulation, however, has not been able to stop abuse and invasions of personal privacy⁵¹.

⁵⁰Sethi (n 7) 147.

⁵¹ Christian Ahlert, 'How Liberty Disappeared from Cyber space: The Mystery Shopper Tests Internet Content Self Regulation' (University Of Oxford 16 December 2014)<<http://pcmlp.socleg.ox.ac.uk/wp-content/uploads/2014/12/liberty.pdf>>

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, which the Indian government announced, set forth several compliance standards for organizations that handle, store, or deal with sensitive personal data or information in their computers, computer systems, or computer networks. The only way to safeguard online privacy appears to be through cyber privacy laws. Legislators must, however, ensure that cyber privacy legislation is as explicit as possible, without room for uncertainty and without opening the door to misuse by the state or regulators. Education of the Indian internet community as a whole about the importance of protecting one's online privacy is another urgent requirement of the hour. The battle for the cause of online privacy will ultimately be won by advancing cyberlaw and public awareness of its protection.

CHAPTER 3-INTERMEDIARY LIABILITY LAWS IN INDIA

3.1 Timeline of Indian Laws dealing with Intermediary Liability.

3.1.1 Information Technology Act, 2000.

3.1.2 Information Technology Act (Amendment) Act, 2008.

3.1.3 Information Technology (Intermediary Guidelines) Rules, 2011.

3.2 The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021.

3.3 Complications brought in by the new rules.

3.1 Timeline of Indian Laws dealing with Intermediary Liability

The way we interact with the world has changed tremendously ever since the Internet came; it has appeared as a boon to society at the present day and age, but with the said boon came a host of problems, including but not limited to hate speech, cyberbullying, fake news and theft of personal data. A good number of these problems stem from online social media platforms. There have also been cases of significant data leaks wherein data stored by these online platforms are breached and sold at the cost of penny chapbooks to analytics companies that target consumers based on such data. The problem is not merely limited to individuals but there is also the problem of intellectual property law violation, for because of the large number of data being uploaded it becomes difficult for these platforms to filter data as a result there have been repeated instances of copyrighted data being uploaded. There is also the problem of counterfeit goods being sold online⁵², thereby maligning the image and goodwill of the company that manufactures the original goods. One may assume since so many breaches are caused due to such platforms then

⁵² Reed (n 9) 47

how are they still flourishing? to understand this question, a better knowledge of the term "intermediary" is required, and it is to be understood how do these platforms get protection from such liabilities by being an intermediary.

The Information Technology Act 2000 is India's mother legislation dealing with the use of computer systems, networks, resources, communication devices, and electronic data and information. The Internet was commercially introduced in India in the year 1996. The growth of the Internet was eventually slow but as it grew, the need was felt to enact laws so as to regulate the content being broadcasted on the Internet⁵³. The following factors fueled this need for immediate enactment of cyberspace laws:

1. India had a relatively well defined legal system that governed the working of the society. However, the Internet signaled the beginning of new and complex legal issues. Despite the brilliant acumen of our drafting technicians, the coming of a new cyberspace regime could not have been anticipated. The emergence of the Internet led to the rise of several new types of legal issues and problems, thereby the enactment of cyber laws became necessary⁵⁴.
2. The existing laws of India could not be interpreted in context to the offences taking place in cyberspace. Thereby to include all aspects of the offences/violations being committed online need for a new cyberspace law was felt.
3. None of the existing laws provided any legal validity or sanctions to the activities in cyberspace. For example, even though emails were being used prominently as a means of communication, they were not "legally" recognized as a means of communication. Even the judiciary at such time could not issue any guidelines for

⁵³Sethi (n 7) 134

⁵⁴Murray (n 11) 213

the domain was new, and there were no specific laws enacted that dealt with the cyberspace.

4. It was noticed that without proper infrastructure, the activities over the Internet could not grow, the internet at that time was rapidly evolving, and the need for regulation became more pressing. A significant aspect of the Internet i.e. E-commerce, was also developing at that point and without proper laws to monitor the cyberspace, eCommerce could not be regulated.

When there was no such heavy usage of the Internet, there was no strict data regulation by the authorities but since the data boom in recent years there has been an increase in the misuse of data leading the spread of fake news, child pornography and riots, therefore, the courts and authorities in the present time are constantly reforming and interpreting laws in a “consumer-friendly” manner so as to impose a stricter sense of liability and responsibility on the intermediaries⁵⁵. In India, there has been a traceable timeline as to how such laws governing Intermediaries have evolved-

3.1.1 Information Technology Act (2000)

While India was caught in the headspace of making a separate enactment for regulation of cyberspace United Nations adopted the UNCITRAL Model Law on Electronic Commerce in 1996 with the aim to provide a common legal platform to the countries to model their domestic laws relating to E-commerce. The model law was not a comprehensive code but provided a basic framework for the nations to build up their domestic laws relating to eCommerce. Inspired by the UNCITRAL law on e-commerce, the Government of India decided to enact a law that would make e-contracts legal, electronic records admissible in evidence and make

⁵⁵ Duggal (n 6) 143

cosmetic changes to some other existing laws. The parliament under Article 253 of the Constitution of India, relying on the resolution of the General Assembly of the United Nations, passed India's 1st cyber law, which became the Information Technology Act, 2000. It received the President's assent on June 9 and was implemented on October 17, 2000.

The objectives of the Information technology act 2000 is to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as electronic methods of communication and storage of information, to facilitate the electronic filing of documents with the Government agencies.

One of the most significant developments and contributions of the Indian Cyber law is that it came up with an entirely new concept for the term "Intermediary". The said concept is very vast, elaborate, wide and comprehensive in its approach, applicability and ambit. Section 2(1)(w) of the IT act, 2000 1st defined the term intermediary, according to it the definition an intermediary is- "with respect to any particular electronic message and means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message" The list provided herein is non-exhaustive and includes ISPs as well as websites generating user-based content. The law relating to intermediaries is elaborated in Section 79 of the Information Technology Act. Section 79 is a code in itself; it is so because it is the only relevant section that provides complete detailed provisions pertaining to the liability of intermediaries and other service providers which fall within the parameters of the Information technology Act, 2000. The Act⁵⁶ states that: *"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,*

⁵⁶ Information Technology Act(2000) s79

rules or regulations made thereunder for any third party information or data made available by an intermediary 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.” Therefore Section 79 of the IT Act, 2000 explained the liability of network service providers. This definition provided a narrow approach as intermediaries were presumed to be liable in the majority of the cases and they were exempted from liability only in certain specified cases.

According to Section 79, Intermediaries were only protected if they were able to prove the absence of knowledge on their part, i.e. they had no active role in the transmission of such content. This section differed in its approach as it shifted the onus of proof from the prosecution to the network service provider. Generally, a person is presumed to be innocent unless proven guilty⁵⁷. However, under Section 79, a different approach was adopted wherein a network service provider was presumed to be guilty unless proven innocent, and the onus of proving innocence was on the network service provider, This section amounted to putting the horse before the cart and gave rise to practical difficulties under the IT Act, 2000. The definition of "third party information" under Explanation 9(b) of Section 79 states that Third party information refers to any information that a network service provider deals with while acting as an intermediary. This information from a third party must unavoidably come from a separate source and be sent somewhere specific. As a result, a network service provider was rendered completely liable for any third-party data he made available on his service. The network service provider in question was only released from liability under two specific circumstances⁵⁸:

⁵⁷ Duggal (n 6) 53

⁵⁸ Kamath (n 8) 183

1. A network service provider is not responsible for any third-party data or information made available on his platform if he can demonstrate that the crime or violation was done without his knowledge. When the word "knowledge" was employed in Section 79, it referred to legal knowledge. It's vital to emphasise that the network service provider had to substantiate that he was unaware of the relevant violation or offence. The law does not specify how or in what manner the network service provider had to demonstrate that he was unaware of the violation or offence. Usually, direct or specific circumstantial evidence can establish the absence of knowledge. But it is also a fact that in most cases, direct evidence about lack of knowledge is not readily available.
2. A network service provider is exempt from liability for any third-party data or information made available by him on his platform if he can demonstrate that he took all reasonable precautions to prevent the commission of the offence or contravention. However, this exception had its own set of issues because it was unclear how a network service provider might prove the excluded circumstance in judicial proceedings before a court of law. Even after the IT Act, 2000 had been in effect for a few years, few individuals were even aware that Section 79 even existed. Later, through a number of cases, the pertinent stakeholder's attention was drawn to the prevalent Section 79 of the IT Act, 2000

3.1.2 IT Amendment Act(2008)

The MMS issue involving Baazee.com⁵⁹ was one of the catalysts for amendment in the IT Act in 2008, it was primarily done to broaden the protection afforded to intermediaries. In this case, an MMS clip containing

⁵⁹ Avnish Bajaj v. State , (2008) DLT 765

sexually explicit content was advertised on Baazee.com (an e-commerce website, a wholly-owned subsidiary of Ebay Inc. USA) and was available for purchase. Avnish Bajaj, the then-Managing Director of Baazee.com, was arrested and criminally charged with provisions of the Indian Penal Code, 1860 and the IT Act, which dealt with acts of obscenity, for selling such content on the company's website. In this case, the Hon'ble High Court of Delhi held that even though a prima facie could be made against Bazeer.com, such a case could not be made against Avnish Bajaj, the owner of Bazeer.com but he could be charged under Section 67 of the IT Act. Avnish Bajaj appealed this order of the Hon'ble Delhi High Court. In 2012 Supreme Court quashed the proceedings against Avnish Bajaj as the company Bazeer.com was not arraigned as a party to the suit. The provision of vicarious liability could only be applied if the company was made a party to the suit. It was only after this case that the need for increasing the scope of Intermediary liability was felt.

The IT Amendment Act of 2008 widened the scope of the term intermediary it now included service providers like cyber cafes, e-marketing, search engines like yahoo and google and even internet service providers. The court also felt the need for properly drafted "Safe Harbor" regulations for intermediaries⁶⁰. Therefore keeping in mind the views laid down by the court Section 79 of the Information Technology Act was amended and a safe Harbor provision was added, this provision provided a Safe Harbor to all intermediaries and not just network service providers. The new provisions protected the intermediaries from "all unlawful acts" thereby not limiting it to selected offences provided the intermediaries complied with the conditions stated in the said provision. To claim

⁶⁰ Sethi (n 7) 317

protection of Safe Harbor the intermediaries had to comply with the following conditions:

- The intermediaries had to comply with the guidelines⁶¹ issued by the central government in this regard and they had to follow the “due diligence” requirement set forth.
- The intermediaries had to ensure that they were not involved in inducing, abetting, conspiring or aiding the commission of an unlawful act.
- The intermediaries had to ensure that upon receiving “actual knowledge” or after being notified by the appropriate authorities to take down infringing/unlawful content.

One of the biggest changes that Section 79 brings in the context of intermediaries is that they have to observe due diligence while discharging their obligations under the IT Act, 2000. The rationale for amending Section 79 of the IT Act and setting up a whole new structure of safe harbor provisions was to bring the laws of India in consonance with EU Directive on e-commerce⁶². The term "intermediaries" was now specifically used to refer to cyber cafes, online auction sites, internet service providers, telecom service providers, network service providers, internet service providers, and web hosting service providers. All service providers would categorically fall within the definition of "intermediary" in its broadest sense. Therefore, in accordance with Section 2(1)(w) of the amended Information Technology Act, 2000, any service provider of any kind of service, whether direct or indirect, that is delivered over a computer platform or that is accessible through a computer network, would also qualify as an "intermediary". A wide number of value-added services today offer various value additions for an efficient and more productive use of electronic/communication devices within the context of

⁶¹ Information Technology (Intermediary Guidelines) Rules (2011)

⁶² Kamath (n 8) 134

the electronic ecosystem. All of the aforementioned service providers will fall under the definition of "intermediary" as well. Due to the growing prevalence of electronic devices, electronic records preserved by the intermediaries are now crucial for both the investigation and punishment of cybercrimes as well as the resolution of disputes.

3.1.3 The Information Technology (Intermediaries Guidelines) Rules, 2011

After the 2008 amendment of the IT Act(2000), Safe Harbor provisions were introduced to provide protection to intermediaries and to regulate such protection the Government of India made the "Information Technology (Intermediaries Guidelines) Rules, 2011" which were mandatory for all the Intermediaries to follow to claim protection under S.79 of the IT act i.e. the Safe Harbor provisions. These were to be read in consonance with the due diligence requirements stated under the IT Act(2000). The requirements to be observed by intermediaries as stated under Rule 3 are-

1. Requirement to publish rule and regulations, privacy policy and user agreement by intermediary.
2. Such conditions need to specify all prohibited acts, that are, "grossly harmful, harassing in nature or unlawful, harms minors, infringes any intellectual property rights, violates any law, is deceiving or misleading, impersonates any person, contains a virus, threatens India etc". The intermediary also needs to make the user aware that violation of such terms may lead to termination of services
3. Intermediaries should not deliberately host or publish information specified in sub-rule(2)

4. Intermediaries to “disable such information within 36 hours and storage of same for 90 days for investigation purposes”.
5. Intermediaries to “provide assistance to authorized government agencies”.
6. Intermediaries to “take all reasonable measures to secure its computer resource”.
7. Intermediaries to “report cyber security incidents to the Indian Computer Emergency Response Team”.
8. Intermediaries to “appoint and publish the details of a Grievance Officer on their website”.

Thus, the IT(Intermediary Guidelines) Rules, 2011 actually mandated that all intermediaries publish Rules and regulations, privacy policy and user agreement for access or use of the intermediary’s computer resources. Various kinds of content has been barred under Rule 3, these are the kinds of content which the rules and regulations and terms and conditions of intermediary must mandatorily inform its users, that they should not use the computer resources of intermediary to host, display, upload, modify, publish, transmit , update or share the s specified information. Although these guidelines were drafted with the best intentions, they failed to clear the air regarding the Safe Harbor provisions and ended up adding to their ambiguity of it⁶³.

Section 79 of the amended IT Act, 2000 has been criticized as being covertly brought about and that the same is not likely to promote the growth of electronic commerce and governance in the country. Some advocates complained⁶⁴ that 2011 rules are outside the scope of Section 79

⁶³ Duggal (n 10) 271

⁶⁴ Duggal (n 6) 47

of the Information Technology Act, 2000 and beyond the scope of IT Act, 2000. It has further been argued that the 2011 rules violate Article 19(2) of the Constitution of India as Rule 3(2) is not in compliance with the same. "Rule 3(2) prohibits inter alia content which is "grossly harmful", "harassing", "invasive of others privacy", "hateful, "disparaging", "grossly offensive" or "menacing", etc. Most of the terminology used are not legal standards, but rather are essentially subjective measures of personal sensitivities. Still other terms, despite being legal, are not included in Article 19. (2). Since the whole structure of intermediary guidelines' i.e. the entire framework is dependent on these extra-constitutional justifications, they could all be overturned. The Intermediary Guidelines, unjustifiably restrict the right to speak and receive information on the Internet, thereby making the restriction unjustified. The Intermediary Guidelines overstep their bounds by classifying as actionable anything that is not itself illegal when transmitted through any other medium.

Four related problems in regards to 2011 rules were pointed out by experts which are as follows:.

- 1) The norms are not well defined and include terms such as “grossly harmful”, “derogatory” and “blasphemous”. The guidelines may have gone beyond the act's delegated powers.
- 2) The regulations may be in violation of the constitutional right to freedom of speech since some of them might not be covered by the kind of reasonable limitations allowed by Article 19(2) of the constitution.
- 3) Whether content is distributed electronically or in physical form, the rules make a distinction depending on that fact. For instance, it may not be permitted to post some content online that is permitted to be published in a daily newspaper.

- 4) The intermediary, rather than the individual who posted the item, is subject to the regulations. If an intermediary does not delete any infringing content after being notified that it has been uploaded on their platform by a third party, even if that third party is not necessarily an official agency, they risk being held liable. The Centre for Internet and Society in Bangalore has sent bogus alerts and discovered that certain intermediaries demonstrate similar behavior. As a result, to avoid such danger, the intermediaries may try to remove even innocent content, thus restricting the free flow of information and speech⁶⁵.

Supreme Court through the case of *Shreya Singhal vs Union of India*⁶⁶ clarified these ambiguities and endorsed the entire Section 79 along with 2011 rules as constitutionally valid. As such, Section 79 of the Information Act, 2000 is a code in itself and must be completely complied with by all intermediaries to enable them to claim exemption from liability for third party data, information or communication link made available or hosted by them.

3.2 The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (Intermediary Rules)

These guidelines were notified by the central government on the 25th of February, 2021 and are the latest amendment relating to the Intermediary liability framework. These new rules⁶⁷ are a step in the positive direction and have brought about some positive changes to the Information Technology (Intermediaries Guidelines) Rules 2011. Intermediaries have now been divided into two categories, i.e. 'social media intermediaries' (SMIs) and 'significant social media intermediaries' (SSRIs). SSMI's are subjected to further

⁶⁵ SFLC, 'Intermediary Liability 2.0: A shifting paradigm'(2019) SFLC <<https://sflc.in/intermediary-liability-20-shifting-paradigm>>

⁶⁶ [2015] SC1532

⁶⁷ Information Technology(Intermediary Guidelines and Digital Media Ethics Code) Rules (2021)

obligations in comparison to SMI's, these rules have brought forward various new due diligence requirements and have also added a mechanism for redressal of grievance by such platforms. On a bare perusal of these guidelines, it can be seen that these guidelines have taken their inspiration from GDPR, 2017 of the European Union, California's CCPA and other such International Data Regimes that have been implemented recently, which govern similar issues at hand. These new rules put forth the appointment of a Chief Compliance Officer whose sole job will be to be the chief point of contact to help law enforcement agencies. The new rules also make it mandatory for the intermediaries to inform the user of their platform if their content is being taken down. The intermediaries now also have to ensure to give appropriate reply to any complainant as to the action taken by them towards the complaint filed. The new rules have also imbibed elements of the draft rules of 2018 and have introduced the rule of monitoring of data so as to Track the first originator of any message. The new rules have also introduced strict penalties for the companies if they fail to comply with these rules these penalties will be discussed further in the analysis part of the paper. Although the government did not take into account any criticisms regarding the original draft rules of 2018 and went ahead with the implementation of these new guidelines.

The new rules⁶⁸ somewhat took these changes into account and have broadened the definition of Intermediary by dividing them into three categories

1. **The original intermediaries** envisaged under Section 2(w) of the IT Act, is a very wide term with the scope to include all entities that would fall within the ambit of these rules. Some additional due diligence requirements have been stated which are:
 - A. **Grievance Redressal-** Complaint system for an online grievance to be established by an intermediary and they are to acknowledge the said complaints within 24hrs of being reported and such complaints are to be disposed of within 15 days of their reporting.

⁶⁸ Information Technology(Intermediary Guidelines and Digital Media Ethics Code) Rules (2021)

- B. Content Takedown-** Where a complaint is made for removal of any inappropriate picture being shared or “Impersonations of them being circulated then the removal of such access material is to be mandated within 24hr of prima facie assessment”⁶⁹.
- C. Privacy Policy-** The intermediaries are now required to serve privacy policies to its users and should set forth user agreements that should clearly outline the terms of use, the intermediaries are now require to serve annual reminders to its users in case if there is any modification to its terms or the intermediaries’ right to terminate the user’s access for using the service in contravention of these terms.
2. **Social Media Intermediaries** are the intermediaries that enable interaction between two or more users. There is no user threshold for such intermediaries and any platform facilitating interaction between two users will fall under this category.
3. **Significant Social Media Intermediaries:** these are the intermediaries who have a registered user threshold of over 50 Lacs; these intermediaries have to adhere to “additional due diligence” requirements i.e.
- A. **Appointment of New In-country employees**⁷⁰- under the new rules the SSMIs need to appoint several in-country employees in the form of “(1) Chief Compliance Officer, (2) a nodal contact person who will be responsible coordinating with the law enforcement agencies 24x7 and (3) a Resident Grievance Officer who will specifically be responsible to oversee the internal grievance redressal mechanism the new guidelines also make it mandatory for SSMI’s to prepare a monthly compliance report wherein they will have to state the complaints made to them and what have they done to deal with the issue stated in the complaint⁷¹ .

⁶⁹ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules(2021) r3

⁷⁰ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules(2021) r4

⁷¹Srinivas Chatti, ‘From Harbor to Hardships? Understanding the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021’ (CAM 24 September 2021) <<https://corporate.cyrilamarchandblogs.com/2021/09/from-harbor-to-hardships-understanding-the->

- B. **Content Screening**⁷²: SSMI's will now have to employ advanced technological measures to take into account any information that relates to the issue of (i) rape, child sexual abuse or conduct, or (ii) any information previously removed following a Government or court order. Content may be taken down for a myriad of reasons including but not limited to -content affecting of threatening national security, content affecting public order or content that might be defamatory or pornographic in nature.
- C. **Identification of First Originator**⁷³- Intermediaries which provide messaging services are now required to identify first originators of information on their platform as required by government or court orders.

3.3 Complications brought in by the new rules

1. **Tracing Requirement**-According to Rule 3(5) of the new rules, intermediaries must make it possible for authorized government agencies to identify the source of information on their platforms. What's most worrying about this requirement is how it will impact intermediaries like WhatsApp and Signal, which offer end-to-end encrypted personal communication services, meaning that not even the service provider has access to the content of messages or information that passes through their platform. The privacy of people using end-to-end encrypted services for their private communication will be compromised if traceability requirements are introduced for those services. This will result in the encryption being broken. In “August of 2017, a nine-judge bench of the Supreme Court in *KS Puttaswamy v. UOI*⁷⁴ (“the Privacy Judgment”), held the right to privacy as a fundamental

information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021-part-iii/>accessed 17 June 2022

⁷² Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules(2021) r4

⁷³ ibid

⁷⁴ [2017] SCC 1

right guaranteed under the Constitution of India”. Since the Supreme court has expressly recognized the right of privacy therefore such requirement may directly impact the citizens.

2. **Filtering requirement:** Intermediaries are required by Rule 3(9) of the new IT Rules to implement automated methods for proactive filtering of illegal information on their platforms. Online middlemen are regarded as conduits of distribution that just serve a technical, non-judgemental function. Given that there are no established definitions of what constitutes "unlawful," this Rule compels intermediaries to examine user-generated content and assess its legality. The Supreme Court of India declared in *Shreya Singhal*⁷⁵ that intermediaries are neutral platforms and do not need to use their own judgement to determine what constitutes legitimate information. This proactive content filtering clause goes against that ruling. Keyword tagging is a significant component of current automated moderation systems, which are then reviewed by humans. Currently, even the most sophisticated automated systems cannot accurately and effectively replace human moderators. This is primarily due to the fact that artificial intelligence is not mature enough to miss subtleties in human communication like sarcasm and irony. Additionally, it should be recognized that cultural variances and overtones have an impact on global communication, which an effective system of content filtering must accommodate. Relying on AI may be shortsighted given the amateurish stage at which it is now operating. The meaning of "grossly harmful/offensive content" changes and evolves along with society. The implication is that algorithms must continuously comprehend the complex social and cultural backdrop that changes among regions.

There are currently no large datasets for this kind of insight from AI research. The use of automatic techniques will boost content removals and account suspensions immediately, which will then result in over-censorship as has been observed globally. The speech of legitimate users (content creators), such as journalists,

⁷⁵ [2015] SC1532

human rights advocates, and dissidents, will frequently be suppressed. The "Content ID" method used by YouTube to identify copyright-violating content has a reputation for excessively restricting lawful content. It will be disastrous for the freedom of speech and expression on the Internet if AI is used without human interaction to identify hate speech, misinformation, disinformation, trolling, etc., which is far more complex than identifying copyrighted material.

3. **Local officer requirement:** All intermediaries with more than 5 million Indian users are required by Rule 3(7) of the New IT Rules now need to, have a permanent registered office with a physical address in India, and appoint a nodal officer and a senior functionary for round-the-clock coordination with law enforcement agencies. Whether this number of users relates to daily, monthly, or yearly users, or to the overall number of registered users, is unclear at the moment. Referencing the user bases of well-known messaging applications is vital in order to comprehend the implications of this criterion. The most widely used messaging app in India is WhatsApp, which has almost 200 million users there. Hike and ShareChat, two relatively recent chat programmes, have 100 million and 25 million users, respectively. The 5 million users included in the Rules account for about 1% of all Internet users in India, which might subject a sizable number of intermediaries to additional compliance standards. This could lead to a large number of startups bearing the burden of the hefty fees associated with formation under the 2013 iteration of the Indian Companies Act.
4. **Use of ambiguous terms:** The New Rules include requirements for a large group of content types deemed "illegal". With such a broad category of content specified using language like "grossly hurtful," "harassing," and "blasphemous," intermediaries would feel pressured to remove even legal content. The terms and wordings used in the rules are vague and there is a risk of over-compliance and excessive screening of social media content. These rules not only apply to social media websites but also to online broadcasting platforms such as Netflix and Amazon prime, regulating such platforms under the light of them being an

intermediary will give the government the power to censor these service providers according to their agenda⁷⁶.

This is the timeline through which law governing intermediaries has evolved in India. The word intermediary, which in the beginning only covered ISPs, now has a whole new definition and includes all sorts of social media platforms, e-commerce websites etc. The dimensions of the safe Harbor provision have also evolved, and now the platforms cannot just claim themselves to be an intermediary and claim protection under it. Still, they need to perform "Due Diligence" on their part. However, with the onset of a new dimension, some new issues have also evolved, of which the laws remain ambiguous.

⁷⁶ Vijay Pal, 'Compliances By An Intermediary Under Information Technology (Intermediary Guidelines And Digital Media Ethics Code) Rules, 2021' (Vaish Associates 9 May 2022) <<https://www.mondaq.com/india/social-media/1189092/compliances-by-an-intermediary-under-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021>>accessed 18 June 2022

CHAPTER 4- JUDICIAL INTERPRETATION OF INTERMEDIARY LIABILITY

4.1 Avnish Bajaj v. State (2008)

4.2 Shreya Singhal v. Union of India (2015)

4.3 In Re: Prajwala (2015)

4.4 Kamlesh Vaswani v. Union of India (2016)

4.5 MySpace v. Super Cassettes (2017)

4.6 Kent RO Systems v. Amit Kotak (2017)

4.7 Christian Louboutin SAS v. Nakul Bajaj (2018)

4.8 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 (2018)

4.9 Sabu Mathew George v. Union of India (2018)

4.10 Google India Pvt.Ltd v. Vishakha Industries Limited (2019)

Indian courts have taken varied stances at different times when it comes to different aspects of Intermediary liability. The following cases sheds some light onn the same:

4.1 Avnish Bajaj v. State (2008)⁷⁷

In this case, a sexually explicit MMS clip that was placed for sale on the e-commerce website Baazee.com . Avnish Bajaj, the former managing director of Baazee.com, was detained and criminally charged under provisions of the Indian Penal Code, 1860, and the IT Act, which dealt with acts of obscenity, for selling such information on the company's

⁷⁷ [2008] DLT 769

website. The Hon'ble Delhi High Court ruled that Baazee.com might be charged with obscenity on the basis of a prima facie case in a petition contesting the criminal charges brought against him. But Avnish Bajaj could not be sued for violating the IPC, but he could be charged with publishing pornographic material online in accordance with Section 67 of the IT Act. According to the court's ruling, owners or operators of websites that allow for listings may need to utilise content filters to demonstrate that they did not intentionally allow for the use of their website to host pornographic material.

Avnish Bajaj filed an appeal against the Section 67 of the IT Act allegation, and the Supreme Court of India annulled the proceedings against him in 2012 on the grounds that the Managing Director's prosecution could not proceed without also accusing the firm. Comparing the IT Act and the Negotiable Instruments Act of 1881 in terms of corporate offences and the subsequent accountability of its officers, the court determined that vicarious liability will only apply when the company is arraigned as an accused party.

The managing director of a corporation was charged for the first time with criminal provisions under Indian penal law and the IT Act for content spread by a third party on an e-commerce platform, making this case significant in India's intermediary liability landscape. Avnish Bajaj was technically excused from responsibility in this case because Baazee.com was not named as an accused party in any case before the High Court or the Indian Supreme Court. The Delhi High Court's ruling in this case had another significant aspect: the court acknowledged the use of content filters to restrict pornographic content and ruled that businesses carry the risk of learning about such content if it manages to get past the filters.

4.2 Shreya Singhal vs Union of India (2015)⁷⁸

This judgement is mostly known for striking down the draconian Section 66A of the IT Act(2000) which provided punishment for use of communication services to send offensive messages. But while striking down Section 66A of the IT Act(2000) the Hon'ble Supreme Court also cleared certain ambiguities present under S.79 of the IT Act(2000), the court held that *“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 relating 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”* The Hon'ble Supreme Court further observed that *“it would be very difficult for intermediaries like Google, Facebook etc. to act when millions of requests are made and the intermediary is then to judge as to which of such requests are legitimate and which are not.”* Thus, through this judgement, the Court laid down its observations regarding the changes to the Safe Harbor provisions brought about by the 2011 guidelines, thereby clearing the air around the term “knowledge” and when the intermediaries are to be held liable.

Although this judgement brought some clarity to the situation the task of creating a perfect balance between providing protection and attributing liability to an intermediary is still a difficult one. In 2018 the IT Minister of India laid down emphasis on the role of intermediaries when hate speech is propagated through their platform, he brought forth the idea of imposing stricter measures, if social media platforms take inadequate measures or delay in taking appropriate action against the accused party. He also believed that IT laws should be revised and amended to respond appropriately to the newly emerging challenges. In the case of My Space vs Super Cassettes⁷⁹(when it was before

⁷⁸ [2015] SC1532

⁷⁹ [2017] SCC 478

the Delhi High Court in 2011) given by the Delhi High court the court held that the Intermediaries are liable for removing only the infringing content in question and cannot be expected to keep vigilance over all such products.

This case is significant from the perspective of copyright because the Delhi High Court division bench overturned a single judge's ruling holding Myspace accountable for copyright infringement in this instance. The division bench said that a chilling impact on free speech can result if intermediaries are charged with identifying illicit information. In this case, the court further clarified the Shreya Singhal⁸⁰ requirement that "actual knowledge" in copyright infringement refers to "specific knowledge," meaning that intermediaries must remove any disputed content if rights holders point out specific instances of infringing content without first obtaining a court order from India⁸¹.

4.3 In Re: Prajwala (2015)⁸²

Sunitha Krishnan, the founder of the Hyderabad-based NGO Prajwala, brought up the problem of sexual assault recordings that are being shared on WhatsApp and other social media platforms in a letter to the Supreme Court of India. She listed the websites hosting the movies and requested, among other things, that the Ministry of Home Affairs be directed to investigate the matter with the help of middlemen like Google, YouTube, and Facebook. After the Supreme Court's social justice bench took suo moto cognizance of the letter, the Central Bureau of Inquiry (CBI) was tasked with conducting an investigation into the recordings. The impacted web portals were asked to be looked into by the Department of Telecommunications and the Ministry of Home Affairs.

⁸⁰ [2015] SC1532

⁸¹University of Washington, 'The Intermediary Liability Project' (2017) UOW <<https://www.law.uw.edu/programs/liabilityresearch/country-reports>> accessed on 7 May 2022

⁸² [2015] SC417

A Committee was set up under the Additional Secretary of the Ministry of Electronics and IT in order to assist and advise the court on the practicality of preventing recordings of sexual abuse and violence from appearing online. Throughout the hearings, the Committee engaged in lengthy conversations with several representatives from various intermediary platforms, lawyers, professors, and members of civil society. The Committee also delivered a two-part report based on its talks that contained some recommendations for limiting the online dissemination of violent and/or sexually explicit videos. Google, Facebook, Microsoft, Yahoo!, WhatsApp, and the Government were all ordered by the court to carry out all recommendations without delay. The Court is still hearing the matter, and a decision is expected soon.

In the case mentioned above, significant questions about the role of intermediaries in limiting the dissemination of violent and suggestive videos were brought up. Retaliation porn and other non-consensual sexually explicit recordings are tied to challenges with drafting rules to address the issue. Notably, a number of the Ajay Kumar Committee's approved recommendations called for restricting search terms with particular keyphrases and prohibiting the source-level upload of violent or sexually explicit movies using hashing and other technologies. The suggestions could become problematic if they are considered as legal requirements with mandatory adherence, even if they are now seen as optional initiatives that stakeholders should work on jointly.

4.4 Kamlesh Vaswani v. Union of India (2016)⁸³

An attorney from Indore filed this public interest lawsuit before the Supreme Court of India, arguing that Sections 66, 67, 69, 71, 72, 75, 79, 80, and 85 of the IT Act are unconstitutional since they are ineffective at addressing the widespread availability of pornographic material in India. He contended that these limitations are pointless because the IT Act was created more to control e-commerce and e-governance than it was to

⁸³[2016] SCC CRI 223

address cybercrimes like the online distribution of pornographic material. The petitioner demanded a number of things, including that watching pornographic recordings be made a cognizable, non-bailable offence, that the aforementioned clauses be declared unlawful, and that a national policy and action plan be developed to combat pornography. Throughout the court proceedings, the petitioner also requested that intermediaries be directed to block access to pornographic content proactively.

While the court appeared sympathetic to the petitioner's allegations, the presiding judges expressed concerns about the technical feasibility and privacy implications of proactive content filtration. The Cyber Regulations Advisory Committee, which was ordered by the Court to look for ways to prohibit access to pornographic content online, tasked the Internet and Mobile Association of India with compiling a list of websites to be blocked. Interestingly, the Indian government closed 857 pornographic websites in August 2015, yet they were all reopened quickly. The Court is considering this issue at the moment.

By restricting access to pornographic content, this case tries to impose proactive content monitoring requirements on online intermediaries once more. It is important to note that the presiding judges acknowledged the technical difficulties in purging the Internet of all pornography. They also mentioned that the government shouldn't have any say in what a person does in the privacy of his or her home. However, the Court has also stated that it is important to prevent the spread of more dangerous types of pornography, such as child porn, and that intermediaries may be required to proactively prohibit access to such content.

4.5 MySpace v. Super Cassettes (2017)⁸⁴

MySpace, a social networking site, was sued in 2007 by Super Cassettes Industries Limited, who claimed that MySpace had violated their copyright. Users of the site may

⁸⁴ [2017] SCC 478

upload and exchange media files, among other things, and it was found that they were spreading SCIL's copyrighted works without permission. SCIL subsequently sued MySpace for primary infringement under section 51(a)(i) of the Copyright Act and secondary infringement under section 51(a) of the Copyright Act (ii). The 2012 order was very concerning since it had reverted the notions of internet intermediary liability to a far earlier era.

Despite MySpace's lack of knowledge regarding specific instances of infringement, the fact that it removed infringing content in response to complaints, and the fact that Super Cassettes neglected to add songs to MySpace's song ID database, the court had found MySpace to be liable for copyright infringement. The need for MySpace pre-screen content rather than relying on post-infringement methods to remove infringing content was deemed the most impractical burden of obligation by the court. This resulted from considering pre-screening to be part of the required diligence. The court ordered MySpace to promptly carry out content removal orders and enjoined it from allowing any uploads of SCIL's copyrighted content⁸⁵. The following excerpts from the judgement clearly sets forth the court's view on this landmark ruling:

“49 Given the supplementary nature of the provisions- one where infringement is defined and traditional copyrights are guaranteed and the other where digital economy and newer technologies have been kept in mind, the only logical and harmonious manner to interpret the law would be to read them together. Not doing so would lead to an undesirable situation where intermediaries would be held liable irrespective of their due diligence.”

⁸⁵Nishith Desai Hotline , ‘Streaming Website Caught Offside’ (Nishith Desai, 17 May 2013) <http://www.nishithdesai.com/information/research-andarticles/nda-hotline/nda-hotline-single-view/article/streaming-websites-caught-off-side-mid-waythrough-the-2014-fifa-worldcup.html?no_cache=1&cHash=7f1906fe691e41d1676c187e8b196a7f>.

“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.”

“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.”

“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.”

This decision strengthened the safe harbor immunity enjoyed by Internet intermediaries in India and is a landmark and forward-thinking decision. In order to reinstate intermediaries' safe harbor immunity even in the face of copyright claims, this judgement helped by harmoniously interpreting the provisions of the IT Act, 2000 and the Copyright Act, 1957. In an effort to find a compromise between free expression and censorship, it also absolved MySpace of the responsibility of reviewing user-uploaded content beforehand⁸⁶.

⁸⁶SFLC, ‘Intermediary Liability 2.0: A shifting paradigm’(2019) SFLC <<https://sflc.in/intermediary-liability-20-shifting-paradigm>> accessed on 11 May 2022

4.6 Kent RO Systems v. Amit Kotak (2017)⁸⁷

The Delhi High Court's single-judge panel declined to ex-ante order intermediaries to screen material that violates intellectual property rules. Amit Kotak (respondent), a manufacturer of water purifiers, violated the intellectual property rights of the petitioner Kent RO Systems by replicating its designs. eBay India Pvt Ltd. further assisted the infringement by enabling the respondent to sell its goods on their platform. eBay India Private Limited requested protection under Section 79 of the IT Act, which exempts it from liability for information, data, or communication links created by third parties as long as those functions are limited to granting access to a communication system.

According to Justice Rajiv Sahai Endlaw's single-judge panel, forcing an intermediary to screen information would constitute "an unreasonable interference with the intermediary's rights to carry on its business." The court further argued that making an online platform screen any type of content would transform their function from that of a facilitator to that of an adjudicator. A third party is only required to remove the content in accordance with Section 79 and the IT Rules of 2011 after receiving a court order or official notification. The court in Kent RO reaffirmed the specific knowledge criteria laid down in Myspace, holding that when an intermediary is made aware of infringing products, they are then required to take those listings down from their websites.

“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

⁸⁷[2017] SCC 321

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.”

Infringement of a design that was registered under the Designs Act of 2000 was at issue in this case. The rights holder demanded that the middleman (eBay) not only delete any products that are currently infringing but also filter similar listings in the future and remove any infringing products that are listed without the owner's knowledge. The court rejected this claim, saying that it was unrealistic to expect intermediaries to have such control over their platforms and that they were only required to remove illegal content upon specific requests.

4.7 Christian Louboutin SAS v. Nakul Bajaj and Ors (2018)⁸⁸

The Delhi High Court established certain guiding principles regarding the responsibility of e-commerce platforms for trademark infringement in November 2018. The plaintiff, Christian Louboutin, a manufacturer of high-end luxury shoes, has registered trademarks in India and exclusively offered its goods for sale through licenced retailers. A website that advertises itself as a "marketplace for luxury brands" is the defendant, Darveys.com. On its website, the defendant allegedly offers for sale fake goods carrying the plaintiff's name, according to the plaintiff.

In addition to offering and selling the plaintiff's products there, the plaintiff said that the defendant utilised the names "Christian" and "Louboutin" as meta tags to drive visitors to its website. This reportedly breached the plaintiff's trademark rights and Mr. Christian Louboutin's personality rights as the brand's creator. The defendant asserted that the goods were genuine and that no infringement had taken place on its end because it was just serving as a middleman and thus qualified for protection under Section 79 of the IT

⁸⁸ [2018] DLT 728

Act. In order to define the role of an online marketplace and the scope of "service" as used in the definition of "intermediaries" under the IT Act, the court listed 26 tasks that an intermediary may complete, including finding the seller, marketing products on the platform, delivering the product to the customer, and using trademarks in meta tags, among other things. The court added that it must be assessed whether the marketplace is taking the required efforts to ensure that the vendors are not involved in illegal activities. Measures cover, among other things, how the conditions of the contracts formed between the platform and the vendors are upheld and what happens when they are not.

The Court opined that *“While the so-called safe harbor provisions for intermediaries are meant for promoting genuine businesses which are inactive intermediaries, and not to harass intermediaries in any way, e-commerce platforms which actively conspire, abet or aid, or induce commission of unlawful acts on their website cannot go scot free. The role of Darveys.com is much more than that of an intermediary. If the sellers themselves are located on foreign shores and the trade mark owner cannot exercise any remedy against the said seller who is selling counterfeits on the e-commerce platform, then the trade mark owner cannot be left remediless.”*

The Court ruled that the characteristics listed above will play a significant role in determining whether an online marketplace or e-commerce website is "conspiring, abetting, aiding or instigating" and, thus, helping in the selling of counterfeit goods on its platform. According to the ruling, when an e-commerce website engages in or conducts its business in a way that would result in the presence of a large number of the aforementioned requirements, it "crosses the line from being an active participant to an intermediary." After considering all of the aforementioned factors, the Court came to the conclusion that Darveys.com cannot be regarded as an intermediary deserving of protection under Section 79 of the IT Act.

This judgement is particularly noteworthy since it was the first time the Court dealt with the issue of trademark infringement by online e-commerce platforms that have asserted that Section 79 of the IT Act exempts them from responsibility. Importantly, the court determined that Darveys.com was not an intermediary and therefore held the website liable for trademark infringement.

4.8 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 (2018)⁸⁹

The terrible incident of a 19-year-old student's death, which was apparently brought on by playing the online game "The Blue Whale Challenge," gave rise to this case. This game required players to complete 50 difficult tasks; failing any of them would end in suicide. Due to the fact that it featured a topic of public interest, the Madras High Court took suo moto cognizance of the case.

The court ordered the government to request that "links" to the Blue Whale game be removed from web portals like Google, Facebook, Microsoft, Yahoo, and Instagram. Google responded by saying that because its app store was managed by the parent company, which was subject to US laws, it was not possible for its Indian subsidiary to delete the content. . It was made clear by Google that their US team was aware of the game and that they would continue to sue businesses that disobey their app store regulations. The court praised Google's answer, and emphasized on how difficult it is for law enforcement to obtain crucial information, and cautioned web corporations against evading their legal commitments. The court further stated that:

"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

⁸⁹ [2017] SC531

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 Central Government was therefore ordered by the court to take the necessary action to place "Over The Top" services within a legal framework, obliging them to abide by Indian law and to provide the necessary information to law enforcement agencies. The court stated that "Methods must to be devised to ensure that those OTTs which could not be brought within such framework are not accessible in India." This case draws attention to a critical sore spot in the ongoing discussion of intermediary liability that affects law enforcement access to material globally, not just in India. The government frequently raises this issue when adopting amendments, such as the latest 2021 Rules, underlining the fact that foreign corporations hide behind source country rules when assisting Indian law enforcement officials. It remains to be seen how tech companies and governments will address the issue of law enforcement's access to information, but any new adjustments must be consistent with free speech and privacy rights.

4.9 Sabu Mathew George v. Union of India (2018)⁹⁰

Doctor and gender activist Sabu Mathew George petitioned before the Hon'ble Supreme Court of India in 2008 to forbid search engines like Google, Bing, and Yahoo from running adverts connected to pre-natal sex determination. The petitioner argued that Section 22 of the Pre-Conception and Pre-Natal Diagnostic Techniques (Prohibition of Sex Selection) Act, 1994 ("PCPNDT Act") was broken by the presentation of these results. The respondents contended in their response that Section 79 of the IT Act protects them since they are "conduits" rather than content providers. It was further stated

⁹⁰ [2018] SCC 229

that although some actions are prohibited by law, both online and offline access to their material nonetheless exists.

For the duration of the proceedings, the court imposed interim orders directing Google, Microsoft, and Yahoo to "auto-block" pre-natal sex determination ads from appearing in search results. The court also developed a list of 40 search terms that would immediately block anyone who attempted to use them. The creation of skilled internal committees to examine and delete content that breaches the law was mandated for search engines. The Central Government was further instructed by the Supreme Court to set up a nodal office for complaints from anyone who comes across anything that resembles an advertisement or might be utilised by any search engine to detect whether a person is a boy or a girl. In this case the nodal agency received valid complaints, the implicated intermediaries were then required to remove the disputed content within 36 hours and notify the nodal agency.

When this petition was ultimately dismissed in December 2017, the apex court issued additional instructions to the newly established nodal agency and expert committee to hold a meeting with assistance from the petitioner's legal team, "so that there can be a holistic understanding and approach to the problem." Additionally, the committee was told to collaborate with Google, Yahoo, and Microsoft to find and apply a "constructive and cooperative way to solve the problem."

The Supreme Court of India ruled in this case that intermediaries were required to prevent illegal content from showing up on their networks. Even after the Supreme Court ruled in *Shreya Singhal*⁹¹ that intermediaries cannot be required to use their own judgement in establishing the legality of content for takedown purposes, the court nevertheless requires intermediaries to actively scan their platforms for illegal content.

⁹¹[2015] SC 1532

Such court rulings add to the uncertainty around the level of care that intermediaries must exercise to safeguard their safe harbor.

4.10 Google India Pvt ltd v. Vishakha industries limited (2019)⁹²

This was an online defamation case against Google being a service provider. In this case, the complainant ran a firm that produced and sold asbestos cement sheets and related goods. Gopal Krishna served as the group's coordinator and regularly posted articles on "Ban Asbestos India," a platform hosted by Google. On November 21, 2008, a piece titled "poisoning the system" was published in the aforementioned group and targeted the complainant, a single manufacturer of asbestos cement products, along with the names of well-known politicians from the nation who had no involvement in the complainant's company's ownership or management. Additionally, another article with the title "Vishaka Asbestos Industries earning gains" was published on July 31, 2008, and both of the aforementioned publications contained defamatory statements about the plaintiff on top of that both of these articles were available on the internet for everyone to read.

In this case the Andhra Pradesh High court held that a network service provider is covered under the definition of an intermediary according to Section 79 of the Information Technology Act, 2000. Therefore the said network service provider may claim safe harbor protection according to the provisions of the IT Act, 2000, provided the said intermediary complies with the requirement stated under sub section(2) of Section 79 of the Information Technology Act, 2000. The court further held that *“As per amended sub section (3) of Section 79, the exemption under sub-section (1) cannot be applied by any court and cannot be claimed by any intermediary in case the intermediary entered into any section (1) in case he fails to expeditiously remove or disable access to the objectionable material or unlawful activity even after recovering actual knowledge thereof”*. In the present scenario even though the 1st respondent brought the infringement

⁹² [2019] SC 1587

to the attention of the appellant, the appellant did nothing to stop the spread of such information through its platform. Therefore in the present case the Appellant could not claim any sort of exemption from the liability on the grounds of them being an intermediary. The said decision was appealed before the supreme court wherein the appeal of google was rejected, and the decision of the Andhra Pradesh High Court was upheld.

From the Judgements stated above, we can see the court's view regarding intermediary liability. While the courts are sympathetic towards the active monitoring requirement for intermediaries, they have a stern view when it comes to material that is criminal in nature, namely child porn, hate speech, etc. These decisions of the Indian courts affirm the view that a more streamlined regulation in reference to intermediary liability is needed as the current laws are quite ambiguous. Because of such ambiguity, the parties are moving to court to interpret such laws, thereby increasing the burden on an already overburdened judiciary.

CHAPTER 5- INTERMEDIARY LIABILITY FRAMEWORKS GLOBALLY

5.1 The European Union

5.1.1 Google v. Spain (2014)

5.1.2 Delfi v. Estonia (2015)

5.1.3 Magyar Tartalomszolgáltatók Egyesülete (“MTE”) and Index.hu Zrt
 (“Index”) v. Hungary (2016)

5.2 The United States of America

5.2.1 Dart vs Craigslist (2008)

5.2.2 Viacom International, inc v. Youtube, Inc (2010)

5.2.3 Matthew Herrick v. Grindr LLC (2019)

5.3 International Doctrines relating to Intermediary Liability

India is not the only country that is trying to tackle the problem of data regulation and the role of Intermediaries; different countries have laid down their own set of frameworks to tackle the problem of Intermediary liability and have set forth the limit of protection that may be attributed to them. There are different approaches to restrict content that may be unlawful, the primary being the “notice and takedown” model- under this model, the intermediaries respond to content takedown notices by the court, government and private individuals. After reviewing the content, they decide whether the content violates any laws and need to be taken down or not; this model leaves some arbitrary power at the hand of the Internet Service Providers who have to act like a judge and decide as to the acceptability of the content on the challenging platform, countries like the USA and South Korea loosely follow this model. The second model of content regulation is the “notice” model- under this model, if a Copyright owner makes a complaint to the intermediary about their copyright content being displayed on the intermediaries website, then the intermediary is to direct such complaint to the party that uploaded such content

in the first place, this model is majorly followed in Canada. The third model is referred to as the “three strikes” model under this model the intermediary upon receiving a complaint from the copyright owner is to send multiple warnings to the subscriber infringing such copyright and after a select number of warnings and review of the complaint, the intermediary removes the disputed content, this model is followed in UK, France etc. To better understand the global position of the treatment of intermediaries we will now look at the framework set forth by The European Union and the United States of America to regulate them:

5.1 The European Union

The EU's member states must create legal defenses for electronic trade under civil and criminal law to advantage specific kinds of internet intermediaries. According to the Information Society and the Enforcement of Directive EU member states are required by laws governing intellectual property to allow owners of intellectual property to request injunctions versus those intermediaries whose services and intellectual property rights are being abused by a third party. The fundamental piece of legislation control is found in Articles 12 to 15⁹³. It puts certain responsibilities on an intermediary and it contains a notice and takedown procedure for the internet intermediaries to follow. Intermediaries are categorized in Articles 1 to 14⁹⁴ under the following heads i.e. “mere conduits” , “caching’ services” and “Hosting services”. Article 15⁹⁵ specifies that since there is no specific requirement for any intermediary to actively keep an eye on the data that they either send or store for any kind of illegal activity⁹⁶.

European Union came up with the General Data Protection Regulation in the year 2017, this regulation started the conversation on the topic of data protection globally but before

⁹³ Directive 2000/31/EC of 8 June 2000 on electronic commerce OJ L 97/21

⁹⁴ Directive 2001/29/EC of 11 July 2001 on Copyright in the Information Society OJ L 83/24

⁹⁵ *ibid*

⁹⁶ Mondschein, C.F., Monda, C. The EU's General Data Protection Regulation (GDPR) in a Research Context, (Springer, Cham, 2018)

this regulation, there were the E-commerce directives, 2000⁹⁷ these directives afforded protection to the intermediaries very much like the Safe Harbor protections afforded to intermediaries in India. This directive also had the provision for individuals to go against an intermediary if any 3rd party was infringing their rights through the use of their platform, Article 12-15⁹⁸ of these directives dealt with the concept of Intermediary liability. GDPR was drafted in a way that it worked smoothly conjointly with the E-Commerce directives of 2000. The GDPR deals with the issue of storage of personal data of the citizens living in the European Union, it regulates the day in which personal data is processed and used by the Online platforms irrespective of them being an intermediary. Article 17 of the GDPR also introduces the “right to be forgotten” which means persons whose data is collected can request that their personal data is erased by the data controller and not processed further. This will include situations where the deal is no longer necessary for its purpose specified, in case of withdrawal of consent or objection of such person or where the processing does not comply with the GDPR. However, the further retention of such data will be lawful in some cases where it is necessary for legal compliance or to exercise or defend legal claims. GDPR requires that a data controller who has made the personal data public is required to inform other data controllers that are processing the data to remove any links to, or copies of that data. Article 31 of the GDPR puts an obligation on the data controller to inform the Information Commissioner Office(ICO) of a personal data breach without undue delay and, where feasible, not later than 72 hours on coming to know of such breach.

GDPR is not limited in application to the European Union and applies globally to any company if they fall under the following categories: “*Where such organisations offer goods or services to data subjects in the EU*”, “*Where such organisations monitor the behavior of data subjects in the EU*”. Therefore GDPR is applicable to any organization that falls under the given bracket whether they are situated in the European Union or not. These regulations widely brought the criteria of appointing a data protection officer who would specifically deal with compliance of these data protection regulations similar to the

⁹⁷ Directive 2000/31/EC of 8 June 2000 on electronic commerce OJ L 97/21

⁹⁸ *ibid*

Chief Compliance Officer requirement of the new Indian IT Rules. Personal Data Protection Bill of 2018 certainly draws a lot of inspiration from these directives especially regulations relating to the online storage of data of the citizens as well as the “right to be forgotten”. GDPR introduced the requirement of Terms and Conditions of the website being expressed in a short manner so that any layman consenting to those terms and conditions would know what his/her data is being used for, this requirement is especially necessary because large scale social media companies put u huge terms and conditions on their website in such a hard language that the citizens fail to understand what their data will be used for and ultimately give consent to their data being used in such shape or form for which they would’ve not agreed if they understood it clearly, a rule of this form has also been inscribed in the Personal Data Protection Bill of 2018. GDPR also imposed huge fines if these Data Processors and Data Controllers failed to adhere to the requirements stated, fines of up to 20,00,0000 pounds or 4 of an Organizations worldwide annual turnover. With the advent of GDPR, the change can be clearly seen and most of the major Websites that fall within the given category have complied with it.

The following cases shows the stance of European courts when it comes to Intermediary Liability:

5.1.1 Google v. Spain (2014)⁹⁹

The Court of Justice of the European Union interpreted the Right to be Forgotten from Articles 12 and 14 of the Data Protection Directive specifically with regard to the delisting of search results by search engines in the precedent-setting case of Google v. Spain. This case established several significant principles in this area. Mr. Costeja Gonzalez, the complainant in this case, sued Google for displaying search results pertaining to the sale of his property for the repayment of social security payments, which occurred ten years ago and was reported in the Spanish newspaper La Vanguardia. He

⁹⁹ Case C-131/12 *Google v. Spain* 2014 ECR II- 2173

requested that the search engine remove these links from its results since they were no longer relevant and were bad for his reputation. During the course of the case, the court came up with the following questions:

1. Are search engines considered to be "Processors/Controllers" of data?

According to Google, it neither processes data nor controls it. It is not the Controller since it does not exert any control over the data and does not distinguish between personal and general data when carrying out its operations. The Court, however, disagreed with this justification. Google was charged with processing, which is defined as gathering, keeping track of, retrieving, organising, storing, disclosing, and making data accessible to the general public. It makes no difference that the data has already been published and has not been changed. The search engine will be the Controller with respect to these activities and cannot be excluded solely on the grounds that it exercises no control over the personal data on the websites of third parties, according to the Court, which also held that the search engine exercises control and determines the purpose and means of the activities it undertakes during processing. The Court further stressed that profiling would be possible if someone entered their name into a search engine and obtained all relevant information about them. Publishers' ability to prevent search engines from getting their data was found to be irrelevant. The responsibility of search engines was distinct from that of data publishers.

2. Duties of Search engine operators

According to Google, in accordance with the proportionality principle, the website publishers are required to decide whether the information should be removed or not since they are in the best position to do so and take further steps to do so. Google additionally argued that being compelled to remove such links would violate both its and the Publisher's basic rights to free speech and expression. The rights of Internet users to information will also be in danger. The

Court underscored the role that search engines play in profiling data subjects and the danger that this poses to people's right to privacy. The court continued the court continued the processing of data cannot be justified only by the financial interests of the search engine. Additionally, one must take into account the rights of other Internet users. The rights of the data subject and those of other Internet users must be balanced by taking into account things like the information's nature, its sensitivity to the data subject's life, the data subject's place in public life, and the public interest. The court also mentioned how easily data can be replicated online, which means that it can end up on websites over which it lacks jurisdiction. Because of this, requiring the simultaneous erasure of the data from the publisher and the publisher's website, or requiring erasure of the data from the publisher's website first, may not be a viable remedy. There may also be circumstances in which the publisher is not covered by the data subject's Right to be Forgotten when it comes to search engines.

3. Scope of Data subject rights

The court was asked to decide whether the data subject might exercise his right to be forgotten by claiming that the information is harmful or that he wants it to be removed after a certain period of time. According to Google, individuals should only be permitted to exercise their right to be forgotten in situations where the processing is in violation of the Data Protection Directive or when there are compelling valid grounds related to the data subject's position. The Court concluded that while the initial collection of data may have been legal, it may later become excessive, erroneous, or irrelevant to the original purpose for which it was intended. The Court further ruled that the information requested to be erased need not necessarily be harmful to the data subject¹⁰⁰.

¹⁰⁰ SFLC, 'Intermediary Liability 2.0: A shifting paradigm'(2019) SFLC <<https://sflc.in/intermediary-liability-20-shifting-paradigm>> accessed 11 May 2022

5.1.2 Delfi vs Estonia, 2015¹⁰¹

One of the most significant decisions in recent years on intermediary liability is the ruling in this case, which raises fascinating problems of both human rights and the law governing intermediary liability in the EU. One of Estonia's largest online news websites was Delfi. Even though Delfi ran a mechanism to control unlawful content inside a notice and takedown framework, readers were nevertheless allowed to comment on the news articles. The road that connected Estonia's mainland to its islands was destroyed by the ferry business SLK Ferry, according to a news report that appeared in Delfi in January 2006. There were 185 user-generated comments on the news story, roughly 20 of which were considered to be threatening and disrespectful to the company's stakeholders. They requested that the comments be taken down and filed a claim for compensation. Delfi complied with its wishes and took down the said comments but refused to compensate them in any manner.

The case was brought before several lower courts before it made it to the Supreme Court in June 2009, which ruled that since Delfi was both the publisher and the original author of the comments on their website, it was not protected by EU Directive¹⁰² and had a duty to take steps to stop unlawful and illegal content from being posted there. The court held that Defamatory statements is not protected by the right to freedom of speech therefore delfi was ordered to provide compensation.

Delfi aggrieved by the said ruling moved to the European Court of Human Rights. The court was to decide whether the order of the Supreme Court holding delfi liable for the comments on said article was infringing upon Delfi's freedom of speech and expression which was available to everyone according to the Convention for the Protection of Human Rights and Fundamental Freedoms. The European Court of Human Rights was to decide upon the balance between "*freedom of expression under Article 10 of the*

¹⁰¹ Delfi v. Estonia App no 64569/09 (ECtHR 2015)

¹⁰² Directive 2000/31/EC of 8 June 2000 on electronic commerce OJ L 97/21

Convention and the preservation of personality rights of third persons under Article 8 of the same Convention¹⁰³ . The ECHR ruled against Delfi on 2013 and therefore Delfi brought the case before the Grand Chamber. The Grand Chamber upheld the decision of the previous courts and held that :

“(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”.

Digital and civil rights activists slammed the ruling for going against directives that shield intermediaries from user-generated content and digital freedom of expression. Additionally, it established a troubling precedent that had the potential to alter the mechanics of intermediary liability framework and online free speech. The Court’s lack of understanding of the position of intermediaries in online media was also heavily criticized.

5.1.3 Magyar Tartalomszolgáltatók Egyesülete (“MTE”) and Index.hu Zrt (“Index”) v. Hungary (2016)¹⁰⁴.

The stance of the European Union in relation to content regulation by intermediaries was seen clearly in the said case. In the given case MTE was a content regulation body and a news website, there was an article about malpractices being followed by a particular real estate company as a result of which the misgivings were brought to light and the

¹⁰³ Directive 2000/31/EC of 8 June 2000 on electronic commerce OJ L 97/21

¹⁰⁴ Magyar Tartalomszolgáltatók Egyesülete (“MTE”) and Index.hu Zrt (“Index”) v. Hungary Application no. 22947/13 (ECtHR 2016)

company was subjected to a lot of harsh comments by the users. The company brought a lawsuit against MTE for harming its reputation. After a judgement by the Hungary court which found MTE liable and didn't allow them the safe Harbor for an intermediary, the case was then brought before the European Court of Human Rights.

The ECHR held that intermediaries cannot be held liable for every content posted on their platform by a third party. Requiring intermediaries to control the content shared by their users would amount to suppression of the right to free speech thereby holding MTE not guilty.

5.2 The United States of America

The Computer Fraud and Abuse Act bans any access to computer network or system which is made without permission and prescribes penalty for any unauthorized access or alteration of information. This legislation is discussed and considered in most online privacy suits. In India, provisions reflecting CFAA are enacted in the IT Act, 2000 wherein Section 43, 66 and 70 in particular deal with unauthorized access issues and prescribe penalties for the same. The Sarbanes-Oxley Act that was enacted in the year 2002 deals with the data retention and preservation issues. SOX prescribes the establishment of the public company Accounting Oversight Board to address corporate liability challenges. This law requires the retention of electronic documents, and their production when summoned by the new Oversight Board.

The USA is one of the originators of the Safe Harbor provisions given to intermediaries. Digital Millennium Copyright Act is the governing act that regulates the protection afforded to Intermediaries. If an Intermediary successfully complies with the notice and takedown procedure stated in the act then they are qualified for protection under this act. Most of the online platforms at the present times have moulded their systems according to the DMCA for eg a platform like youtube where millions of videos are uploaded by users on a daily basis. However, youtube over time has created its own filter system that

doesn't let any user upload any form of explicit content on its platform and actively monitors it is impossible for a platform that operates at such a large scale to monitor each. Every video uploaded therefore it introduced the copyright strike system wherein a person whose copyright has been infringed can report such infringement to you-tube and youtube after reviewing the said content sees whether the content is "fair use" of the artist's original work and if it's fair use then the video is not removed. Still, if it is not covered under fair-use then the said video is removed. DMCA was one of the guiding legislation that made other countries consider providing protection to their intermediaries.

5.2.1 Dart vs Craigslist (2008)¹⁰⁵

The most popular online classified ad service in the US is Craigslist. Advertisements for jobs, housing, the selling of various goods, and other services are posted on the website. Even though Craigslist's terms and conditions expressly forbid the posting of criminal activity, the advertisements nevertheless featured a space for "erotic services." State and municipal police enforcement were interested in the "erotic services" area. It was discovered that some users were promoting illicit services in this section. An order to remove the advertisements for prostitution and other illegal acts prohibited by state law was sent to Craigslist in March 2008 by the attorney general of Connecticut on behalf of the attorney generals of forty other states.

Craigslist and the Attorney Generals came to an agreement in November 2008 to take actions to impede illegal listings on the erotic services section, but not to totally delete them. Later, Craigslist reported a 90% decrease in its listings for erotic services. A sheriff for the county in Illinois named Thomas Dart sued Craigslist four months later, saying that the website had violated Illinois state law by creating 21 categories and offering a word search feature, which significantly interfered with the public's health, safety, peace,

¹⁰⁵ [2008] 665 F. Supp. 2D 961

and welfare. In the end, Craigslist prevailed in that dispute by relying on CDA Section 230(c)(1). According to the court, Craigslist is protected from claims of wrongdoing by third parties because it is an Internet service provider i.e an intermediary. This case was held to be big victory for online intermediaries as it further upheld their right to free speech.

5.2.2 Viacom International, Inc v. Youtube, Inc (2010)¹⁰⁶

A landmark case in this regard that clearly defined the limit of protection being provided to intermediaries was the case of Viacom is one of the world's biggest entertainment networks that makes and produces shows across several countries in 2007 it brought a lawsuit against youtube for Copyright Infringement and sought damages of One Billion USD. It alleged that over 1 lakh videos of the shows made by Viacom were uploaded on youtube and these shows were original work of Viacom and thereby protected under Copyright Laws. Since Viacom was not the only company whose content was being uploaded on youtube without consent, this led to many class-action lawsuits being filed against youtube for copyright violation¹⁰⁷.

These lawsuits tested the mettle of the DMCA Safe Harbor regulations, the courts ruled that it is not possible for a platform like youtube where millions of videos were being uploaded every day by third parties to closely monitor each and every video so as to ensure that no copyright violation was being done, youtube had devised its own takedown system through which parties could directly approach the platform and get the said video taken down, therefore the court held that youtube being an intermediary was protected under the umbrella of DMCA Safe Harbor regulation and thereby not liable to pay

¹⁰⁶ [2010] WL 2532404

¹⁰⁷Miguel Helft, 'Judge Sides With Google in Viacom Suit Over Videos' (New York Times, 24 June 2010)<http://www.nytimes.com/2010/06/24/technology/24google.html?_r=0> accessed 11 June 2022

damages. Later, Viacom challenged the said decision, but ultimately, the lawsuit was negotiated and settled between the parties outside of the court¹⁰⁸.

This decision of the Circuit Court of Appeals of the United States showed the extent to which Safe Harbor provision protects the intermediaries and is considered one of the most landmark cases in this regard. With regards to the issue of Data Protection of the citizens each and every state of the USA have the authority to make their own laws in this regard, unlike the European Union's GDPR which collectively applies to all the members of the European Union.

California is one of the first states to come up with its own data protection regime in the form of the California Consumer Privacy Act, this act is very similar to the GDPR, 2018 enacted by the European Union. It protects the privacy of the citizens residing in the state of California and lays down conditions similar to that in the GDPR, 2018 such as the right of the user to remove his/her data from a website, the rule regarding companies need to inform the user for what purpose their data is being used. With each passing day more and more companies are complying with the rules laid down under the CCPA so that they can function in the region without any hitch or problem¹⁰⁹.

5.2.3 Matthew Herrick v. Grindr LLC (2019)¹¹⁰

Herrick claimed that his ex-boyfriend created a number of phoney Grindr profiles that falsely identified him and led to identity theft. The mimicking profiles received more than a thousand responses. Then, Herrick's ex-boyfriend would pose as Herrick and direct potential suitors to Herrick's place of employment and residence. The fake profiles were

¹⁰⁸ Jonathan Stempel, 'Google, Viacom settle landmark YouTube lawsuit' (Reuters, August 2011) <<http://www.reuters.com/article/us-google-viacom-lawsuit-idUSBREA2H11220140318> (120) 17-CV-932 >Accessed 11 June 2022

¹⁰⁹ SFLC, 'Intermediary Liability 2.0: A shifting paradigm'(2019) SFLC <<https://sflc.in/intermediary-liability-20-shifting-paradigm>> accessed 11 May 2022

¹¹⁰ [2019] 17-CV-932

reported to Grindr, but according to Herrick, Grindr only responded by sending an automated reply. Herrick filed a lawsuit against Grindr, accusing the company of negligence, intentional infliction of emotional distress, false advertising, and misleading business practices for allowing him to be impersonated and turned into an unintentional beacon for stalkers and harassers who were liable to him due to the app's flawed design and failure to police such behavior on the app¹¹¹. Herrick's argument that Grindr is not an interactive computer service as that term is defined in the CDA was denied by the court. The court determined that all of Grindr's product responsibility, negligent design, and failure to warn claims were based on another app user's information. The "neutral aid" that Grindr offered to his ex-boyfriend included algorithmic filtering, aggregation, and presentation features. This kind of help is available to both good and bad users of the app. The court emphasized that whether to remove content or allow it to remain on an app is an editorial decision, and holding Grindr accountable for its decision to leave the impersonating profiles in place would hold Grindr accountable as if it were the publisher of that content.

5.4 International Doctrines relating to Intermediary liability

The Manila Principles

These principles are some guidelines set forth to outline safeguards that countries must apply to their legal framework regarding intermediary liability. The idea behind the manila principles is to harmonize the relationship between the rights of an intermediary and the rights of the user and to keep these rights in line with international standards such as the UNDHR (Universal Declaration of Human Rights) and UNGPBH (United Nations Guiding Principles on Business and Human Rights). They broadly lay down 6 principles which are as follows:

1. Safe Harbor provision for intermediaries to protect them from liability for the content of a third party.

¹¹¹ Andy Greenberg, 'Spoofed Grindr Accounts Turned One Man's Life Into a 'Living Hell'' (WIRED Feb 20, 2019) < <https://www.wired.com/2017/01/grinder-lawsuit-spoofed-accounts/>> accessed 7 June 2022

2. Restriction of content only when the judicial system makes such order.
3. Unambiguous laws relating to notice and takedown of content and the procedure for such need to be clearly established.
4. Content being restricted should pass the threshold of necessity and proportionality.
5. There needs to be due process in relation to policies relating to the restriction of content.
6. The implementation of the laws and policies relating to intermediaries must be transparent and accountability must be attributed to the right parties.

The world community has so far reacted favourably to the Manila Principles. Other initiatives created best practises to safeguard fundamental rights that intermediaries may use in their terms of service. For instance, the Dynamic Coalition for Platform Responsibility, which operates under the auspices of the IGF, intends to define a set of sample contractual clauses¹¹². This clause should adhere to the UN "Protect, Respect, and Remedy" Framework and the UN Guiding Principles on Business and Human Rights, as adopted by the UN Human Rights Council. To "enable Internet users to readily identify the platform-providers who are dedicated to safeguarding the protection of human rights in a responsible manner," appropriate digital labels should indicate the inclusion of these model contractual clauses in the Terms of Service of chosen platform providers. In order to establish a global framework to safeguard and advance freedom of expression and privacy in information and communications technologies, the GNI once more brought together a multi-stakeholder group of businesses, civil society organisations, investors, and academics. Participants in the GNI, including Facebook, Google, LinkedIn, Microsoft, and Yahoo, vowed to abide by a number of fundamental principles, including the GNI Principles, Implementations Guidelines, and Accountability, Policy & Learning Framework. Another project that encourages optimal practises and openness among online intermediaries is Ranking Digital Rights. This

¹¹² Trevor Cook, 'Online Intermediary Liability in the European Union' [2012] JIPR 17

project rates Internet and telecommunications providers based on how well they uphold users' rights, such as their right to privacy and freedom of speech. The first project's report from November 2015 included rankings for 16 businesses across 30 distinct metrics in several nations. Companies received scores ranging from 65 to 13%. For their public promises and openly stated rules affecting users' freedom of expression and privacy, the majority of corporations received poor grades.¹¹³ In order to highlight potential chilling effects and provide alternatives, a number of initiatives have been looking into notice and take down methods. Lumen archives takedown notices. to encourage openness and to make takedown method research easier.¹¹⁴

India follows most of the principles laid down above in spirit. India has a conditional safe Harbor provision for intermediaries. The intermediaries are required to take down content only after a government or court order. The only place where India lacks when it comes to the following of manila principles in the ambiguities aspect of it as there is no strict framework for intermediaries to follow and the condition of “due-diligence” to be followed by intermediaries is not very clear. With the coming of the new 2021 amendment, the laws have become more ambiguous and somewhat arbitrary as it now gives the government the power to take data regarding the originator of the information. There is also a lack of due process in a case when the content of a creator is taken down, there is no proper redressal mechanism and process to help such creator. So what can be seen is that India does comply with some of the Manila principles but is still lacking in certain respects¹¹⁵.

CHAPTER 6: RECOMMENDATIONS AND CONCLUSION

¹¹³ Giancarlo F. Frosio, ‘Internet Intermediary Liability: WILMAP, Theory and Trends’(2017) 13(1) IJLT <<https://www.ijlt.in/journal/internet-intermediary-liability%3A-wilmap%2C-theory-and-trends>> accessed on 14 may 2022.

¹¹⁴ Julia Reda ‘Proposal For A Directive Of The European Parliament And Of The Council On Copyright In The Digital Single Market’(Julia Reda, 12 August 2019)<https://juliareda.eu/wp-content/uploads/2019/02/Copyright_Final_compromise.pdf>accessed 23 May 2022 .

¹¹⁵ Kamath (n 8) 63.

6.1 Recommendations

6.2 Conclusion

6.1 Recommendations

With the increase in the number of people using the internet and the fast rate at which this number continues to grow, it is a need of the hour that a proper ecosystem that establishes the liability of Intermediaries be enforced in India. With the coming of 4g in India, it has become the country with the most significant number of users present online and using these e-commerce and social media platforms daily. Due to the general population's lack of online media literacy, the Indian Online ecosystem has exploded with all types of harmful content, be it propagation of hate speech, spreading of disinformation, and some severe offences such as Revenge porn and Child pornography. With no proper data protection and intermediary laws, these offences keep rising at a breakneck pace. Apart from the said problems, there is also the concern of users' privacy for companies like Facebook and other analytics companies are actively selling the data of Indian citizens. Such data is being used to manipulate the life choices of the citizens by bombarding them with targeted advertisements when they use the internet.

What users see on the internet is determined by their browsing habits, so it is high time now that fact-checking be put into place and the data of the Indian citizens be protected; we have seen that through the application of GDPR and CCPA that these intermediaries have the power to protect data of its users but due to no proper laws regulating them, they are actively exploiting data of the Indian users. The new regime should take heed of the following things

- There is a need for a new set of data protection laws to ensure that the data of the Indian citizens are not sold freely to third parties resulting in the exploitation of Indian users. Just like under GDPR, the citizens know what the data is being used for; likewise, the Indian citizens should also have the right to know where their information is being stored or with whom it is being shared¹¹⁶.
- There is a need for a regulation that enforces the “Right to be forgotten” so that it is ultimately in the hand of the user to add or remove their data from a website as per their requirement. There have been various judgements in India wherein the courts have ordered websites to remove a citizen's personal data from their platform;. However, the judicial intent is there; there is a need for a codified law which sets down the conditions wherein a citizen may ask for their data to be removed without taking the long route of going to a court and getting it removed; such law should also state the procedure to be followed in such cases. This will not only ensure a citizen’s right to be forgotten but will also reduce the burden of the judiciary, which is currently flooded with many such cases.
- Social media Intermediaries like Facebook often hide controversial permissions in the black letters of their terms and conditions. These terms and conditions sometimes extend to 100s of pages. An average day-to-day user cannot go through the whole terms and conditions and understand the same, therefore, a rule needs to be put in place stopping the companies from doing so and making them state clearly and in unambiguous terms what the data will be used for and what are the users ultimately consenting to. This practice has already started with the coming of GDPR, and the Terms & Conditions shown to European Union citizens are different than that in India. Companies have complied with GDPR and if India comes up with a similar policy, the companies won’t have any significant

¹¹⁶ Mondschein, C.F., Monda, C. *The EU’s General Data Protection Regulation (GDPR) in a Research Context*, (Springer, Cham, 2018)

problem in amending their Terms and Conditions in accordance with the said legislation.

- A strict guideline should be set forth that mandates the deletion of user data once the purpose for which it was collected is complete. Such law should ensure that the intermediaries inform the user about the period and the purpose for which data is collected and should inform the user once the information is deleted from their platform.
- There is a need for less ambiguity in the language used when defining data to be blocked and deleted by a website. In unambiguous terms, the law should state what sort of data will be considered illegal and needs to be taken down; this will help the intermediaries design AI-based tools that will not allow any such data to be uploaded. Everything is not black and white on the internet, there will always be a grey area in terms of content uploaded on a website, but through practice, a fine line may be achieved.
- Currently, no strict laws regulate the “right to privacy” aspect of data. Such laws are to be given utmost priority, and such privacy needs not only from the intermediaries but from the government itself. In the current amendment, this aspect is the most debated and controversial, for the government under this amendment has indirectly given itself the right to see the data of any user on the prospect of that user being the originator of a given piece of information, plus the wording used in this regard is very ambiguous thereby making it difficult to interpret. Plus, companies like WhatsApp use end-to-end encryption technology making it almost impossible to see what information is being exchanged between users; removing the safeguard of end-to-end encryption will have severe consequences and ultimately do more harm than good.

- Presently, there is no proper redressal forum that only deals with data protection and intermediary liability. A new regulation is needed that should put in place an appropriate grievance mechanism not only on the part of the intermediary but also on the part of the government. Under the latest amendment, the provision for the appointment of a Chief Compliance Officer is a step in the positive direction, but attributing personal liability to them when charges against them can be both civil and criminal is erroneous and needs to be changed. The government should set up a separate department that deals explicitly with issues related to data breaches and other grievances that the users may have while using such platforms. This department should also focus on the problem of citizens being targeted through their browsing history and their choices being influenced by using such data.
- There is a need for a guideline so that due process can be established in relation to content regulation, i.e. when a creator's content is removed from a platform, he must have the right to contest such removal and put forth his arguments towards the defence of their content. Presently platforms like youtube do not allow small creators to defend themselves if their content is removed; this leads to a violation of their freedom of expression, and many competitors use this exact broken mechanism to get the content of their rivals deleted from a platform.
- Presently the criteria of an intermediary are comprehensive; therefore, there is a need for a regulation that properly sets out the requirements that will make an organization an intermediary, and any organization that falls out of the given criteria and actively starts influencing the content on its platform should not be afforded protection under the Safe Harbor provisions.
- Presently there is no clear-cut mechanism for how content on a platform is to be taken down. Therefore new guidelines need to be set forth; these guidelines should specify the process through which content on an intermediary's platform is

to be taken down. It should clearly state if and how many warnings are to be given to an uploader if the content infringes trademark or copyright. An emergency mechanism also needs to be set up that could be used in cases of serious breach such as hate speech and child pornography that will actively affect the conscience of the society at large and may lead to the commission of a crime or cause unrest.

- Intermediaries should be encouraged to work hand in hand with media agencies to curb the problem of the spread of misinformation and to help these intermediaries fact-check the information being put up on their platforms.
- Apart from introducing new rules and regulations to curb the problems, the government should focus on educating the citizens about the uses of the internet and provide its citizens with adequate social media literacy.

6.2 Conclusion

After a detailed analysis of the position of intermediaries in India, we can see that a new regime setting forth clearly the law on intermediary liability is the need of the hour. Before the 4g Internet revolution, when access to the internet was a privilege, the way these social media platforms and e-commerce platforms dealt with the Indian market was very different; their position was truly that of an intermediary, i.e. social media websites connected different users worldwide while acting just as a medium of that interaction whereas e-commerce websites only brought buyers and sellers together, with their platform only serving as the medium through which both these parties exchanged goods and money. But ever since the 4g revolution, the presence of Indian citizens online increased by leaps and bounds and with it, there was a dramatic rise in the misuse of these platforms, hate speech and the spread of disinformation became rampant, and there was no body of law to fact check such individuals spreading hate or misinformation. The

intermediaries failed to keep a check on their platforms and, whenever questioned, brought up the protection provided under the Safe Harbor provisions. The intermediaries not only failed to regulate their channel properly but also developed a business out of it; these platforms started running advertisements on their websites and started promoting products of companies that paid them money; to top it all, these advertisements were not run randomly but were run based on the analytics presented by users browsing behavior. This method was morally wrong and harmed the individuals by guiding them to particular articles or products based on their browsing behavior, thereby highly violating individuals' right to privacy. Cases also came to light wherein political parties worldwide were shown to have paid large sums of money to these intermediaries so that they could manipulate people into voting for a certain organization by only showing their positive side, thereby highly influencing the election results of a country. A very big example is the Myanmar military using Facebook(as discussed in the introduction)¹¹⁷ to spread their anti-Rohingya ideology; they systematically targetted Facebook posts as most of the citizens of Myanmar considered Facebook as the main source of online information, and by making hundreds and thousands of posts, the military actively hid the atrocities Rohingya Muslims were going through. When the companies started to involve themselves so deep into the lives of the people, then they could no longer be said to be a neutral third party between two individuals as now they are actively influencing the behavior of a citizen; thereby, they should lose the protection afforded to them as an intermediary. The platforms acting as intermediaries had a duty to uphold the protection of the users on their platform. Still, they failed to do the required amount of work and even started making money out of the private data of the users. The personal data protection bill framed in 2018 have broadly reflected the principles of the European Union's GDPR¹¹⁸. The Rules provide that a body corporate(as defined under Section 43A of the IT Act, 2000) that possesses or deals with sensitive personal data information in a computer resource that it 'owns, controls or operates in the course of its commercial activity, are under an obligation to maintain reasonable security practices to protect such

¹¹⁷ Paul Mozur, 'A Genocide Incited on Facebook, With Posts From Myanmar's Military' (New York Times, 15 October 2018) <<https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html>> accessed 17 April 2022

¹¹⁸ Mondschein, C.F., Monda, C. *The EU's General Data Protection Regulation (GDPR) in a Research Context*, (Springer, Cham, 2018)

personal information. Rule 3 of the said rules explains that ‘sensitive personal information includes such personal information that may comprise of passwords, financial information, health-related information, biometric information or other information stored or processed under lawful contract or otherwise. Rule 4 of the said rules obligate every ‘body corporate’ to provide a privacy policy and disclosure information, *among other things*, type of personal information collected, purpose and disclosure information will only be made after consent is obtained through a letter, fax or e-mail and such collection is for a lawful purpose and only to the extent necessary for the purpose and will be retained only till purpose is achieved. It also entitles a consumer to decline from parting with any requested information or to withdraw its consent and correct or amend any information provided. However, unlike the EU, Data Protection Directive, Information Technology(Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 do not prescribe a supervisory authority and its prior permission before collection of any personal data by a body corporate. Also, law on use of cookies to collect sensitive data or through traffic data or display in public directories and rights of netizens has not been specifically addressed in these rules.

Although Indian rules provide an opt-in approach before a body corporate collects sensitive personal information of a netizen, it fails to provide any law regarding a user's consent as to mode or method of collection, which is missing from Rules 5 and 6 of the said rules. Regarding unsolicited advertising, the rules presently do not prescribe an opt-in or opt-out approach. These are certain aspects that require supplemental laws or clarification o existing laws relating to the privacy protection regime in India.

With innovation in Information Technology and continuous efforts to frame more straightforward laws to decide on cross-border B2B and B2C disputers, many hybrid models of e-commerce will grow phenomenally soon. While stronger consumer protection laws will encourage and promote e-commerce activity, strict data protection principles and privacy norms will make cyberspace more reliable and secure for e-

commerce transactions¹¹⁹. We learnt through our discussions that the Indian Legal Regime needs a few additional consumer protection provisions to protect consumer interests, particularly at the contract formation stage, and to safeguard netizens' sensitive personal data and information. It is, therefore, beneficial to formulate these other laws for steady growth of e-commerce activity and to promote its optional deployment across all horizontal and vertical sectors of industry or e-business.

Copyright Protection.

On the internet, the protection of intellectual property has a significant bearing on the growth of e-commerce. Although it may be easy to detect infringement of intellectual property rights on the internet, law enforcement effectively poses a challenge while combatting violation of intellectual property rights in the digital space. Therefore, it is of pertinent importance to awareness of intellectual property rights through seminars and workshops, emphasize on IP registration and deploy other protection measures, including technological measures to protect IP. Industry associations could play a vital role in spreading awareness of the benefits of adopting a robust IP protection strategy for all e-businesses. Corporate entities must be sensitized by allocating reasonable resources to develop, monitor and protect their IP assets, including registering domain names bearing their trademarks in time to avoid cybersquatting¹²⁰.

Major IP infringements in the IT sector occur at the user level, wherein they consume such content through the intermediary's website. Therefore social sensitization is required to respect the rights of the original creator of IP and build a robust regulatory

¹¹⁹ Mukul Sharma, 'Safe Harbor Protection for E commerce platforms' (CAM, 15 February 2021) <<https://corporate.cyrilamarchandblogs.com/2021/07/safe-harbor-protection-for-e-commerce-platforms/>> accessed 9 May 2022

¹²⁰ SFLC, 'Intermediary Liability 2.0: A shifting paradigm'(2019) SFLC <<https://sflc.in/intermediary-liability-20-shifting-paradigm>> accessed 17 June 2022

regime that deters intermediaries and criminals through stringent legal enforcement actions to combat IP infringements. Using computer evidence to prosecute IP offences can play a vital role in tackling IP infringements in cyberspace¹²¹. Assessing IP piracy risk and deploying strategies to prevent and combat prevailing piracy will benefit all stakeholders, users, and corporate, government authorities as IP infringements make them vulnerable to legal, financial and security risks, and governments suffer a substantial loss on taxes. Thus, a multi-faceted approach is required to adequately protect intellectual property rights in cyberspace.

Data Protection

The freedom of speech and expression on the internet in India is guaranteed by Article 19¹²². It is regulated by reasonable restrictions permitted by the Constitution of India and the IT Act, 2000. The law on privacy of personal data guaranteed by Article 21 of the Constitution of India and data protection is an area which is still evolving in India, and the legal framework is being strengthened to enhance data security and privacy in the online space through enacting appropriate rules under the IT Act, 2000. Despite being free, the internet, in many ways, is still territory-specific regarding freedom of speech and privacy laws on the internet. In this setting, legal framework, enforcement provisions, jurisdiction issues, and the role of e-crime conventions become indispensable, particularly in cross-border issues. Another emerging challenge in the internet space is growing convergence in technologies, in the form of, internet messaging to mobile handsets, where telecommunications and broadcasting laws will need to be re-analyzed and aligned with laws for internet communication, including law of interception, law against spamming, and other laws to protect privacy and data of netizens.

¹²¹ 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) <<https://spicyip.com/2019/02/saregama-pa-rdon-me-you-have-the-wrong-address-on-the-perils-and-pitfalls-of-notice-and-takedown.html>> accessed 19 May 2022

¹²² The Constitution of India(1950) art19

Recognizing this state, a new concept of net neutrality is gaining importance. Net Neutrality advocates that internet transmissions and law relating thereto should remain neutral irrespective of content and origin of communications flowing over internet. Recent examples where net neutrality principles did not permit the continuation of certain web-based services are Facebook's "free basic plan" and Airtel's 'zero plan'. This debate addresses the pros and cons of net neutrality, related issues of surveillance powers and censorship of the internet and ISP liability and its impact on further growth of the internet. A homogenized internet or convergence law will eventually be required to govern cyberspace. Yet, at this point, it remains to be tested how much net neutrality can be *de facto* achieved.¹²³

The new 2021 IT law amendment is a step in the positive direction wherein more liability is being attributed to intermediaries, and the meaning of the term intermediary has been made wider. Still, these new rules come with their fair share of ambiguities and are not up to the international standards; they have certainly taken inspiration from Frameworks in other countries. Still, they have not applied them correctly in the Indian scenario. The intermediaries dealing with the messaging option between users now have the requirement to provide the government with information regarding the "originator" of the message being shared on their platform. The rules also put up the requirement of automated screening of messages¹²⁴; these requirements extend beyond the traditional meaning of the term due diligence and have transgressed into the problem of breach of privacy as there is a threat of conversations between private individuals being shared. This requirement of tracing and identification of users is incompatible with end-to-end encryption technology employed by messaging applications like Whatsapp¹²⁵. The terms and wordings used in the rules are vague, and there is a risk of over-compliance and

¹²³ Ankoosh K Mehtat, 'What about the Intermediary? Demystifying the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021' (SCC Online Blog, July 12 2021) <<https://www.scconline.com/blog/post/2021/07/12/information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021-3/>> accessed 13 June 2022

¹²⁴ Whatsapp, 'Explanation of the end-to-end encryption used by WhatsApp on its service' (Whatsapp 10 November 2018) <<https://faq.whatsapp.com/en/android/28030015/>> accessed 11 June 2022

¹²⁵ Whatsapp Report, 'Intermediary Liability & Freedom of Expression'(Whatsapp 17 March 2021)<<http://cis-india.org/internetgovernance/intermediary-liability-and-foe-executive-summary.pdf>> accessed 11 June 2022

excessive screening of social media content. These rules apply to social media websites and online broadcasting platforms such as Netflix and Amazon prime; regulating such platforms in the light of them being an intermediary will give the government the power to censor these service providers according to their agenda. Currently, there are no privacy laws enacted in India, and the bill related to protecting the privacy of citizens, i.e. the Personal Data Protection bill, has not been passed yet; therefore, with the enforcement of such rules, there is a severe concern of privacy violation and online activity being traced. The government has stated that the companies will be required to submit data regarding the “originator” of information only in cases of “serious concerns” such as messages inciting violence or harming the image of any women in India. However, such statements are not official rules mentioned in the amendment and cannot be trusted entirely as previously sedition laws have been misused to suppress dissent¹²⁶.

The provision of employing new In-country employees being added is also a cause of the problem as the provision clearly will hold those employees liable for the failure to perform due diligence on behalf of the company; no person would want to undertake such a risky role as the personal safety of the said person will be at stake owing to the enormous size and reach of these platforms. The liability attributed to such employees is also criminal in nature, wherein punishment can range from 2-7 years in prison; therefore finding an employee willing to undertake such big responsibility and willing to undertake such risks involved is a herculean task and also goes against the global norms of human rights.

The government failed to include the IP framework that goes along with intermediary liability. In India, e-commerce platforms are growing at a fast rate; with the rise of e-commerce platforms, there is growth in the selling of counterfeit goods. There have been more than one instance wherein counterfeit goods of branded companies are sold on these

¹²⁶ University of Washington, ‘The Intermediary Liability Project’ (2017) UOW
<<https://www.law.uw.edu/programs/liabilityresearch/country-reports>> accessed 7 June 2022

platforms; the consumer spends money believing the goods to be from a specific company. When the goods arrive and are not up to the mark, the company's goodwill is affected, and revenue is also lost as a result. These online platforms take shelter under the Safe Harbor provision and state that they don't have any active role in choosing the goods sold by the seller and to who the goods are being sold to, therefore since they have no active participation in the whole process therefore they are exempted from liability. There was no regulation in relation to such practices in e-commerce platforms, albeit it has been seen in various cases that these platforms sometimes actively promote a seller. Still, there is no proper redressal mechanism for removing those goods. These regulations also failed to bring about due process concerning a creator whose content is taken down. YouTube, and other platforms have now become a source of income for many people and their whole income depends on the content they create, now, in many cases, their competitors or other users deliberately report their content to get it removed even when there is no copyright infringement. In such a case, the content creator is at a loss as there is no proper grievance redressal mechanism for them where he can prove and justify that the content in question does not affect anyone's copyright.

Therefore India needs to follow a systematic approach by firstly bringing a law to protect the private data of the users in India and with such data protection law, a new law that clearly highlights the rights and liabilities of an Intermediary when working in the Indian online ecosystem should also be enacted. A proper framework needs to be established so that no one can have access to a user's sensitive data, be it the intermediary or the government itself. All flak can't be directed only towards an intermediary it's high time that Social media literacy be promoted so that users do not fall for online hate propaganda or fake news being spread on a platform. Notice and takedown policy should be interpreted in case of sensitive issues and where the Image or Copyright of a company is at stake. A proper redressal mechanism also needs to be set up for cases wherein a creator's content is removed on malicious grounds or without actually analyzing it; presently, there are no redressal mechanisms wherein the creator may justify his content or present his side of the argument. With the technology improving day by day, the rate at which data is being shared will only increase; therefore, to protect the privacy of its

citizens and to ensure that proper liability is attributed to the intermediaries, a new Intermediary Liability Management Ecosystem needs to be established to deal with the dynamic population of a country like India.

BIBLIOGRAPHY

Books

Andrew Murray, *Information Technology Law*(1st edn, Oxford University Press 2010)

Chris Reed, *Computer law* (2nd edn, Universal Law Publishing 2010)

Karnika Seth, *Computers, Internet and New Technology Laws*(2nd edn, Lexis Nexis 2016)

Mondschein, C.F., Monda, C. *The EU's General Data Protection Regulation (GDPR) in a Research Context*, (Springer, Cham, 2018)

Nandan Kamath, *Computers Internet & E-commerce* (5th edn, Universal Law Publications 2014)

Pavan Duggal, *Cyber Law* (1st edn, Universal Law Publication 2014)

Pavan Duggal, *Law of intermediaries* (1st edn, Universal Law Publication 2016)

International Instruments

1948 Universal Declaration of Human Rights

1966 International Covenant on Civil and Political Rights

2011 United Nations Guiding Principles on Business and Human Rights

Reports

Article 19, '*Responding to 'hate speech': Comparative overview of six EU countries*'
(Article 19 7 March 2018)

<[https:// www.article19.org/wp-content/uploads/2018/03/ECA-hate-speech-compilation-report_March-2018.pdf](https://www.article19.org/wp-content/uploads/2018/03/ECA-hate-speech-compilation-report_March-2018.pdf)>

Google, '*Government Requests to Remove Content, Google Transparency Report*' (Google 26 February 2019), <<https://transparencyreport.google.com/government-removals/overview?hl=en>>

Google, '*Search Removals under European Privacy Law, Google Transparency Report*' (Google 19 June 2018) <<https://transparencyreport.google.com/eu-privacy/overview?hl=en>>

Law Commission, *Report of Parliamentary Committee on Subordinate Legislation* (Law Com 31, 2013)

University of Washington, '*The Intermediary Liability Project*' (2017) UOW <<https://www.law.uw.edu/programs/liabilityresearch/country-reports>>

Whatsapp Report, '*Intermediary Liability & Freedom of Expression*' (Whatsapp 17 March 2021) <<http://cis-india.org/internetgovernance/intermediary-liability-and-foe-executive-summary.pdf>>

Online Journals and Articles

Abby K. Wood, Ann M. Ravel, 'Fool Me Once: Regulating "Fake News" and other Online Advertising' (2018) 122(7) SCLR <<https://southerncalifornialawreview.com/2018/09/01/fool-me-once-regulating-fake-news-and-other-online-advertising-article-by-abby-k-wood-ann-m-ravel/>>

Andrew Mathew, 'Russia "meddled in all big social media" around US election' (BBC, 17 June 2019) <<https://www.bbc.com/news/technology-46590890>>

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

Ankoosh K Mehtat, 'What about the Intermediary? Demystifying the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021' (SCC

Online Blog, July 12 2021)

<<https://www.sconline.com/blog/post/2021/07/12/information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021-3/>>

Aria Thaker, ‘Indian politicians are now flocking to an unlikely “no English” social network’ (Quartz 11 November 2018) <<https://qz.com/india/1414241/sorry-facebook-indias-bjp-and-congress-flock-to-sharechat/>>

Arstechnica, Study of French “three strikes” piracy law finds no deterrent effect”(Arsttchnica,4July 2014) <<http://arstechnica.com/tech-policy/2014/01/study-of-french-three-strikes-piracy-lawfinds-no-deterrent-effect/>>.

Article 19, ‘Internet Intermediaries: Dilemma Of Liability(2013) <https://www.article19.org/data/files/Intermediaries_ENGLISH.pdf>

B. Sinha, ‘SC orders CBI probe into rape videos circulated on WhatsApp’ (Hindustan Times 25 June, 2016) <<http://www.hindustantimes.com/india/sc-orders-cbi-probe-into-rape-videos-circulated-on-whatsapp/story-6OUIIUVqd0nVqKHrXPxyeK.html>>

Christian Ahlert, ‘How Liberty Disappeared from Cyber space: The Mystery Shopper Tests Internet Content Self Regulation’ (University Of Oxford 16 December 2014)<<http://pcmlp.socleg.ox.ac.uk/wp-content/uploads/2014/12/liberty.pdf>>

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) <<https://spicyip.com/2019/02/saregama-pa-rdon-me-you-have-the-wrong-address-on-the-perils-and-pitfalls-of-notice-and-takedown.html> >

EDPS, The History of the General Data Protection Regulation, (EDPS 20 January 2018) <https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en>

FIPR, ‘Implementing the EU Copyright Directive’ (FIPR, 12 June 2011)<<https://www.fipr.org/copyright/guide/eucd-guide.pdf>>

Giancarlo F. Frosio, 'Internet Intermediary Liability: WILMAP, Theory and Trends'(2017) 13(1) IJLT <<https://www.ijlt.in/journal/internet-intermediary-liability%3A-wilmap%2C-theory-and-trends>> accessed 14 may 2022

Gilbert, David "Youtube will broadcast copa America live", online: (3 June 2011) <<http://www.trustedreviews.com/news/youtube-will-broadcast-copa-america-live>>

IndiaSpend, 'Child-lifting rumours caused 69 mob attacks, 33 deaths in last 18 months'(Business Standard, 1 February 2017)

<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>

Jillain York, 'European Commission's Hate Speech Deal With Companies Will Chill Speech' (EFF 19 June 2019) <<https://www.eff.org/deeplinks/2016/06/european-commissions-hate-speech-deal-companies-will-chill-speech>>

Jon Russell, 'Hike unbundles its messaging app to reach India's next wave of smartphone users' (Techcrunch 4 Dec 2018) <<https://techcrunch.com/2018/01/16/hike-unbundles-its-messaging-app/>>

Jonathan Stempel, 'Google, Viacom settle landmark YouTube lawsuit' (Reuters, August2011)<<http://www.reuters.com/article/us-google-viacom-lawsuit-idUSBREA2H11220140318> (120) 17-CV-932 >

Julia Reda 'Proposal For A Directive Of The European Parliament And Of The Council On Copyright In The Digital Single Market'(Julia Reda 12 August 2019)<https://juliareda.eu/wpcontent/uploads/2019/02/Copyright_Final_compromise.pdf>

Kate Andrews, 'Right to be forgotten by Google should apply only in EU, says court opinion' (The Guardian 10 January 2019)

<<https://www.theguardian.com/technology/2019/jan/10/right-to-be-forgotten-by-google-should-applyonly-in-eu-says-court>>

Mathew Connor, ‘EU agreement with tech firms on hate speech guaranteed to stifle free expression’ (Index On Censorship 11 May 2016) <<https://www.indexoncensorship.org/2016/05/eu-agreement-tech-firms-hate-speech-guaranteed-stifle-free-expression/>>

Miguel Helft, ‘Judge Sides With Google in Viacom Suit Over Videos’ (New York Times 24 June 2010) <http://www.nytimes.com/2010/06/24/technology/24google.html?_r=0>

Miguel Helft, ‘Judge Sides With Google in Viacom Suit Over Videos’ (New York Times, 24 June 2010) <http://www.nytimes.com/2010/06/24/technology/24google.html?_r=0>

Mukul Sharma, ‘Safe Harbor Protection for E commerce platforms’ (CAM, 15 February 2021) <<https://corporate.cyrilamarchandblogs.com/2021/07/safe-harbor-protection-for-e-commerce-platforms/>> accessed 9 May 2022

Natasha Duarte, Emma Llanos, Anna Loup, ‘Mixed Messages? The Limits of Automated Social Media Content’ Analysis, Presented at the 2018 Conference on Fairness, Accountability, and Transparency (10 January 2017) <<https://cdt.org/files/2017/12/FAT-conference-draft-2018.pdf>>

Natasha Singer, ‘The Week in Tech: How Google and Facebook Spawned Surveillance Capitalism’ (New York Times 1 March 2019,) <<https://www.nytimes.com/2019/01/18/technology/google-facebook-surveillance-capitalism.html>>

Nishith Desai Hotline , ‘Streaming Website Caught Offside’ (Nishith Desai, 17 May 2013) <http://www.nishithdesai.com/information/research-andarticles/nda-hotline/nda-hotline-single-view/article/streaming-websites-caught-off-side-mid-waythrough-the-2014-fifa-worldcup.html?no_cache=1&cHash=7f1906fe691e41d1676c187e8b196a7f>.

Paul Mozur, ‘A Genocide Incited on Facebook, With Posts From Myanmar’s Military’ (New York Times, 15 October 2018) <<https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html>>

SFLC, 'Intermediary Liability 2.0: A shifting paradigm'(2019) SFLC
<<https://sflc.in/intermediary-liability-20-shifting-paradigm>>

Shivnath Thukral, 'Bringing More Transparency to Political Ads in India' (Newsroom 12 December 2018) <<https://newsroom.fb.com/news/2018/12/ad-transparency-in-india/>>

Srinivas Chatti, 'From Harbor to Hardships? Understanding the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021' (CAM 24 September 2021) <<https://corporate.cyrilamarchandblogs.com/2021/09/from-harbor-to-hardships-understanding-the-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021-part-iii/>>

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

Vijay Pal, 'Compliances By An Intermediary Under Information Technology (Intermediary Guidelines And Digital Media Ethics Code) Rules, 2021' (Vaish Associates 9 May 2022)
<<https://www.mondaq.com/india/social-media/1189092/compliances-by-an-intermediary-under-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021>>

Whatsapp, 'Explanation of the end-to-end encryption used by WhatsApp on its service' (Whatsapp 10 November 2018) <<https://faq.whatsapp.com/en/android/28030015/>>