INTERMEDIARY LIABILITY IN THE DIGITAL AGE: BALANCING CORPORATE RESPONSIBILITY AND CYBERSECURITY

Manisha Debnath (LL.M. in Corporate Law) ICFAI University, Dehradun

ABSTRACT

Due to digital growth, people are rapidly shifting to the digital world, leading to a significant expansion of the digital landscape. As a result, intermediaries such as social media platforms and internet service providers have increased liability and responsibility. When it comes to responsibility, they are tasked with protecting individuals' personal data, among many other obligations. This article will examine the legal frameworks outlined in the IT Act regarding intermediary liability and will focus on the legal frameworks of other countries, such as the Digital Services Act in the EU and Section 230 of the Communications Decency Act in the United States. It will also explore the safe harbor provision, which protects intermediaries from liability. The article further highlights the challenges of balancing corporate responsibility with cybersecurity, including the issues intermediaries face regarding fake news, hate speech, and data privacy in the digital age. The article analyzes the legal and ethical considerations involved in protecting privacy and free speech. Finally, it suggests better cybersecurity practices and greater transparency to create a safe and fair online environment.

Keywords: Intermediary, Liability, Cybersecurity, privacy, free speech.

Introduction

Intermediaries serve as a medium through which one message is transfer from user to another. just as the postal services provide us the infrastructure to deliver a letter from one address to another, intermediaries today, with their digital infrastructure facilitates us to deliver a message seamlessly in todays digitally connected world. Intermediaries such as WhatsApp, Facebook, Twitter, Instagram, etc. An intermediary is not limited to social media platforms. After the 2008 amendment, several other categories were added.

Section 2(w) defined 'intermediary' of the IT Act, 2000 as "any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, web-housing service providers, search engines, online payment sites, online auction sites, online market places and cyber cafes".[1]

Section 79 of the IT Act, 2000[2] discusses the liability of intermediaries. Section 79(1) says when a third party shares a post or content using an intermediary, the intermediary holds no liability for the content being shared. Section 79(2) and (3) limit the immunity of intermediaries. It states that intermediaries will only be granted immunity if they have no unlawful involvement in the particular content shared by a third party. Section 79(3)(b) establishes a "notice and take down" regime, requires intermediaries to remove unlawful content when notified by the government. if an intermediary fails to remove the unlawful content, it will loss its immunity.

Legal Framework

USA

Section 230 of the Communications Decency Act, 1996 states that internet service providers will not be held liable for content uploaded by users. Additionally, platforms are permitted by the Communication Decency Act to delete particular content under certain circumstances, the intermediary will not be liable for this. Intermediaries are only liable for the content they create, not for the content uploaded by users. The new rules includes intermediaries must identify the

[1] Malvika Kapila Kalra, Intermediary Liability Under the Information Technology Act: Time for an Amendment?, Bar & Bench, (July 28, 2019),
[2] Section 79, Information Technology Act, 2000,

sender of flagged posts. Platforms must practice due diligence and take action on flagged content within 36 hours.

European Union

In the digital sphere, the European Union is seen to be the most active legislature. The E-Commerce Directive, which was passed in 2000, governs intermediaries' responsibility for material created by third parties in the EU. Several gaps and uncertainties emerged in the directives. To address these challenges, the EU introduced a new liability framework called the Digital Services Act. The new Act introduced several changes and established new secondary liability for online intermediaries. Furthermore, the "Good Samaritan" clause was introduced, which added guidelines on how intermediaries can enhance content control. New obligations were also established regarding intermediary liability, and the role and power of digital platform regulations in the EU were defined. The E-commerce Directives established the Safe Harbor Principle. It also discussed who this principle would apply to. The Safe Harbor Principle applies to mere conduit service providers, caching providers and hosting providers.[3]

India

Information Technology Act, 2000

Before the IT Act (amendment) of 2008, Section 79 addressed intermediaries' liability, but it was not entirely clear. However, there were no exceptions granted to any particular kind of Intermediaries. Before, network service providers were subject to section 79.

In the case of Google India Pvt Ltd. Vs Vishakha Industries 2009

Fact of the case – A defamatory article was posted in a google group. The aggrieved party, (Vishakha) notified google about this content, but google did not take any action. In response, google stated that google group is controlled by its parent company, google LLC, and that it has no control over it. Google also claimed that it is not liable because the amendment to section 79 came into effect after the complaint was made.

[3] An Analysis of Intermediary Liability in India and the European Union, Manupatra,

Judgment – intermediaries were granted limited protection under the pre-amendment version. The revised provision and associated regulations would apply. The court noted that google was could not claim immunity under the pre-existing section 79.[4]

After amendment Section 79 of the IT Act, 2000[5] discusses the Safe Harbor principle. The "safe harbor" idea was introduced to protect intermediaries, specifically revising section 79. which provides conditional immunity to intermediaries. Section 79(1) says that if a third party posts any content, the intermediary will not be held liable for it. Section 79(2) and (3) outline the conditions under which intermediaries receive immunity. This applies when their role is passive and purely technical. If an intermediary is involved in any unlawful activity, they cannot claim immunity. Section 79(3)(b) states that intermediaries must remove infringing content if notified by the government.

In the case of Shreya Singhal vs Union of India

Fact of the case – two girls were detained in 2012 after posting on Facebook that they were expressing their displeasure about the bandh in Mumbai after Bal Thackeray's death. They have arrested under section 66A of the IT Act, 2000.[6]

Judgment – the court referred to several judgments highlighting the importance of freedom of speech and expression.

In the case of Romesh Thappar vs State of Madras, 1950 "Freedom of Speech lay at the foundation of all democratic organizations".

In sakal papers pvt. Ltd. & ors vs Union of India, 1962, a Constitutional Bench of this Court "A democratic constitution that allows for changes in the composition of legislatures and the government must protect the right to freedom of speech and expression of opinion".

Court also refer a foreign case Whitney vs California, 71 "Liberty should be viewed as an aim in itself and any attempt to restrict free speech should be justified explanation that doing so would lead to grave consequences".

[4] An Analysis of Intermediary Liability in India and the European Union, Manupatra,
[5] Section 79, Information Technology Act, 2000,
[6] Section 66A, Information Technology Act, 2000,

The Supreme Court declared that section 66A of the IT Act as unconstitutional and invalidated it on the grounds that it restricted free speech.

Section 69A of IT Act, rule 2009 was held intra – vires to the Constitution of India.

After the IT Act's section 79(3)(b) was read down, it was determined that section 79 was valid.

Intermediary Guidelines and Digital Media Ethics Code Rules, 2021

Rule 3(2)(7) of the Intermediaries Guidelines Rules lists the categories of information that will be considered illegal content if posted online.

Rule 3(4)(8) it states that the affected person can request the intermediary to remove the content under Rule 3(2). The intermediary must remove the content within 36 hours. If the intermediary fails to remove the content within the time limit, it will lose the protection of the "Safe Harbor" principle.

Challenges in the digital age

All individuals have the right to freedom of speech and expression provided in the Indian constitution. In the digital era, intermediaries like social media platforms provide a space for individuals to express their views. However, some people misuse this right to spread fake news and hate speech. Now, we have all become dependent on social media and tend to believe every posted news as real. Nowadays, people intentionally or unintentionally share fake news on social media just to make themselves famous. A lot of fake job advertisements run on social media and we believe them as a real and we fall victim to scams. In 2025, A new scam is being reported where a message from a well-known person's WhatsApp account asks you to resent an OTP that was mistakenly sent to your number. If you resent the OTP, hackers can take control of your mobile. Nowadays, people use AI to quickly create fake content that has a significant impact on society.

Sometimes government exert pressure to delete specific information, while intermediaries try to protect freedom of speech and expression. Moderation of content is still a challenges face by the intermediaries. Intermediaries in this digital age also face significant challenges related to data privacy and breaches. Everyday, new cyberattacks occur, making it difficult to protect user data. Cyberattacks like ransomware, hacking, DDoS attacks etc. social media has billions

of users, with billions of posts, video and comments share every day. Identifying illegal content among them becomes a challenging task for intermediaries. Even AI-based moderation can lead to errors.

Corporate Responsibility vs Cybersecurity

- **Corporate Responsibility**

  a. In the digital age, when companies store and collect users' sensitive information, it becomes their responsibility to safeguard personal data such as financial information, health records, operational data, personally identifiable information, payment card details, employee data and government and regulatory information.

  b. Companies should have a clear policy on data collection, storage and sharing for users.

  c. To protect user's sensitive data, companies must comply with existing Indian laws such as the DPDP Act and the IT Act.

  d. If a cyberattack or data breach occurs in a company, it is the company's responsibility to notify users about it.

  e. Another responsibility of companies is to provide training to employees about cyberattacks so they can protect from it. Cyberattacks like phishing, malware, social engineering attacks.

- **Cybersecurity Measures**

  a. To prevent cyberattacks, companies must keep their computer system update and use strong security software.

  b. Companies should collaborate with law enforcement agencies.

  c. Companies can provide training to employees about new cyberattacks.

Legal and Ethical Considerations

- **Human Rights concerns**

Human rights are a broad topic and have always been a subject of ongoing discussion. In today's digital world, protecting privacy has become an important task. Intermediaries like Facebook, WhatsApp and Instagram are facing challenges in safeguarding user's privacy. In India, the right to privacy is not directly explain in the Constitution of India, 1950 but has been interpreted and derived from Article 21, which states that "No person shall be deprived of his life or personal liberty except according to procedure established by law"[7]. Over the year, the Indian Supreme Court has interpreted Article 21 to included privacy as a fundamental right, it is expanded through judicial interpretation rather than direct constitutional provision.

In the landmark case *K.S. Puttaswamy vs Union of India,* it was decided that privacy is a fundamental right under Article 21 of the Constitution, which guarantees the "right to life and personal liberty".

As per section 17(2)(a) of the DPDP Act, 2023[8], the government is granted certain exemptions, allowing it to collect and process the personal data of citizens for purposes related to national security, the integrity or security of the state.

This can also lead to the misuse of personal data.

- **Freedom of speech and expression**

Freedom of speech and expression is a major legal issue on social media. Social media is a platform where users express their views. However, it also contains a lot of content such as hate speech, disinformation, and offensive material. Article 19(1)(a) of the Constitution of India guarantees the "right to freedom of speech and expression"[9]. Article 19(2) outlines reasonable restriction on "freedom of speech and expression"[10]. In India, the *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules,* 2021 require social media companies to remove illegal content within 36 hours of receiving a complaint.

Despite the fact that freedom of speech is a "Fundamental Right", government and social media platforms find it difficult to strike a balance between allowing free speech and preventing harm,

[7] Article 21, Protection of life and personal liberty, Constitution of India,
[8] Section 17(2)(a), Digital Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India),
[9] Article 19(1)(a), Constitution of India,
[10] Article 19(2), Constitution of India,

unchecked communication on social media can lead to the spread hate speech and false information.

- **Due diligence by platforms**

1. Intermediaries must publish their rules, privacy policy and user agreement so that users can understand what is allowed and what is not.

2. Users must be informed about what they are not allowed to share :-

    a. One cannot claim someone else's belongings as their own.

    b. One cannot promote illegal content such as harmful, obscene or defamatory material

    c. One cannot upload content that harms children.

    d. Anything that goes against the law.

    e. Violates someone's copyright or patent.

    f. Misleads people or share offensive content.

    g. One cannot work using someone else's name.

    h. Uploading viruses or hacking tools is not allowed.

    i. Nothing should be done that threatens national security or public order.

3. An intermediary will not knowingly publish any illegal content. However, if any data is automatically store without human control, it will not be considered a violation.

4. If an intermediary becomes aware of illegal content on its platform, it must remove it within 36 hours. It must also retain records for 90 days to assist in investigation.

5. If a user does not follow the rules, the intermediary can block their access and remove the illegal content.

6. Intermediaries must operate in accordance with all rules and regulations.

7. If any legal agency or police require data for an investigation, the intermediary must provide it properly.

8. The intermediary must maintain strong system security as per the IT Rules,2011.

9. In case of a cyberattack or any security issue, it must be reported to the Indian Computer Emergency Response Team (CERT-IN).

10. Intermediaries are allowed to make technical changes for security purposes, but they cannot intentionally modify their system settings in a way that violates the law.

11. The intermediary must provide the name and contact details of a Grievance Officer on its website. If users face any issues, they can file a complain with the officer, and a solution should be provided within one month.

Recommendation

1. Nowadays, everyone uses social media, so intermediaries should create awareness about cyberattacks on their websites and inform users about how to stay safe from them.

2. Platforms should make their content moderation policies accessible to the public and give explanations for any material removals or blockings. In compliance with natural justice principle, a right to be heard must be assured prior to removing user material.

3. It is crucial that intermediaries make investment in cybersecurity infrastructure, such as secure data storage, encryption. In abidance with relevant data protection legislation, such as the DPDP Act, 2023, resilient data privacy measures have to be lay into place.

Conclusion

In the digital era, everyone uses social media platforms, e-commerce websites, search engine. Intermediaries like Facebook, Instagram, Twitter, WhatsApp, Flipkart, Amazon and YouTube are widely used. While using these platforms, intermediaries collect and store users' personal data. This creates a responsibility for them to properly safeguard users' privacy and personal data. Also, intermediary play an crucial role in shaping public opinion, sharing information and

influencing social and political discourse. They must take strong measures against hate speech, fake advertisement and illegal content. Additionally, to protect users from cyberattacks. Intermediaries should adopt a robust cybersecurity mechanism to safeguard digital infrastructure and provide users with a healthy digital environment.