SCLS Law Review Vol. 4. No.3 [September 2021], ISSN (Online): 2523-9236, ISSN (Print): 2523-9228
S.M. Shakib & Noor Afrose, Intermediary Liability in Internet, 42-49

Intermediary Liability on the Internet: Adequacy of Bangladesh's Legal Framework on Cyber Crime

S.M. Shakib
Student of LL.B. (Hons), 3rd Year, Bangladesh University of Professionals
Noor Afrose
Student of LL.B. (Hons), 3rd Year, Bangladesh University of Professionals

Abstract

In the last several years, the internet has entered every aspect of modern life. Internet intermediaries have become an integral part of the daily routine, providing access to, hosting, exchanging, and storing third-party content. Many of today's most powerful corporations, such as Facebook, Google, and YouTube, serve as information intermediates. Social networking companies did not have the capability or expertise a few years earlier to establish adequate safety measures and combat cybercrime. Technology has advanced in the following decade, and internet intermediaries now have the tools to combat cybercrime. However, due to the lack of adequate legal instruments regarding internet intermediaries in Bangladesh, intermediaries are not willing to execute a significant change and prevent cybercrime. The focal point of this paper is to highlight the gaps in the current legal framework dealing with internet intermediary liability. Another important area this paper will address is the necessity of internet intermediary liability to combat those crimes. Finally, this paper provides recommendations for necessary modifications in the current legal framework such as the incorporation of comprehensive definitions, implementation of the notice-to-down and notice-to-notice procedures for monitoring unauthorized content, and so forth to encompass deficiencies.

1. Introduction

The Internet has become entrenched in human life. Even though the internet is a very powerful tool for everyday life, the rapid advancement of technology has also resulted in the emergence of new types of online crime, which are often termed as 'cybercrime'. Like other countries, Bangladesh is also going through rapid digitalization in every sector. Therefore, there is an increasing concern about cybersecurity. A study conducted by a UK-based body Comparitech ranked Bangladesh sixth among sixty countries for the worst cybersecurity in the world [1], which proves the lack of an effective cybersecurity system.

Effectively combating cybercrime and an effective cybersecurity system requires a collective responsibility and significant cooperation between law enforcement agencies and the private sectors. Internet intermediaries (ISPs, Facebook, Google, YouTube, etc.) have a special role to play in this collective responsibility. Therefore, countries around the globe have been imposing liability on internet intermediaries by their laws. Bangladesh, following the footsteps of other countries, has incorporated rules regarding intermediary liabilities in the municipal laws. This

[1] Shanjida Hossain, 'Cyber security, a growing crisis for youths' *The Financial Express* (Dhaka,28 July) <https://www.thefinancialexpress.com.bd/education/cyber-security-a-growing-crisis-for-youths-1595441724> accessed 2 August 2021.

study aims to examine the competency of the existing laws regarding internet intermediary liability in Bangladesh. In this paper, the laws of other jurisdictions have also been analyzed and compared with the laws of Bangladesh.

2. Concept of Intermediary Liability and the Intermediaries

In Jaani Riordan's remarks, the term "internet intermediary" is an unsatisfactory notion.[2] There is almost no legal definition of the word "internet intermediate" in legal instruments.[3] An online intermediate can be regarded as a canal that facilitates content to stream from one user to another over the online platform.[4] Intermediary liability refers to how accountable an intermediary is for the contents it maintains and provides. Moreover, it alludes to a company's duty for content that the authorities regard to be immoral, illegal, or detrimental. When it emerges as to who should be regarded as internet intermediaries, ISPs and web hosting companies that offer the structure, browsers, and social media platforms that serve substance and facilitate correspondence will fall under this umbrella.[5] In our country, whoever identifies as an intermediary is stated in section 79 of the Information and Communication Technology Act, 2006. The network service provider will be regarded as an intermediate, according to section 79.[6] However, the current definition does not refer to an internet intermediary.

3. Necessity of Intermediaries in Preventing Cyber Crime

All Internet stakeholders have a collective responsibility to make cyberspace secure. Internet intermediaries have a special role to play in combating cybercrime. They can be participants in investigations by supplying information or data to law enforcement agencies with a warrant. In Bangladesh, the rate of online sexual harassment and cyber pornography is quite high. In Dhaka, 70% of women who are subjected to online harassment are between the ages of 15 and 25, and the majority of them have been subjected to sexual harassment in online, cyber pornography, and blackmail.[7] Intermediaries can develop advanced Artificial Intelligence (AI) features to censor offensive, obscene, and unlawful content. For instance, recently Instagram has launched a feature that will prevent users from reading potentially harmful comments by screening offensive words, phrases, and emojis.[8]

In the case of serious offenses such as terrorism, drug trafficking, pornography, and crimes against the state, the intermediaries have an important role to play by permanently or temporarily disabling electronic data. In October 2020, a video of a woman in Noahkhali's Begumganj Upazila being gang-raped was published and circulated on social media.[9] The

[2] Jaani Riordan, *The Liability of Internet Intermediaries* (OUP 2016).
[3] Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (OUP 2020) p 54.
[4] Rebecca MacKinnon, Elonnai Hickok, Allon Bar, and Hai-in Lim, *Fostering Freedom Online: The Role of Internet Intermediaries (*UNESCO Publishing 2015) p 19.
[5] ARTICLE 19, 'Internet intermediaries: Dilemma of Liability' (ARTICLE 19, 2013) <https://www.article19.org/data/files/Intermediaries_ENGLISH.pdf.> accesed 2 August 2021.
[6] The Information and Communication Technology Act 2006, ss 79.
[7] Tribune Desk, '70% of women facing cyber harassment are 15-25 years in age' *Dhaka Tribune* (Dhaka,24 September 2019) <https://www.dhakatribune.com/bangladesh/dhaka/2019/09/24/70-of-women-facing-cyber-harassment-are-15-25-years-in-age> accessed 6 August 2021.
[8] Staff Correspondent, 'Instagram launches feature to tackle hate speech, abuse' *Dhaka Tribune* (Dhaka, 21 April,2021) <https://www.dhakatribune.com/world/2021/04/21/instagram-launches-feature-to-tackle-hate-speech-abuse> accessed 4 August 2021.
[9] Staff Correspondent, 'Outrage as woman gang-raped, filmed' *The Daily Star* (Dhaka, 5 October 2021) <https://www.thedailystar.net/frontpage/news/outrage-woman-gang-rapedfilmed-1972769>accessed 4 August 2021.

High Court Division instructed the authority to take down the video from social media immediately.[10] It would not be possible if there was no intermediary liability.

In cases of cyberbullying and cyber harassment, women and children get victimized the most. According to a new regional study conducted by a multinational mobile phone company, 49 percent of school pupils in Bangladesh have been victims of cyberbullying in some form.[11] According to research done by the human rights organization Ain O Shalish Kendra in five districts of Bangladesh, a high number of children have been subjected to various types of online harassment during the Covid-19 pandemic.[12] Therefore, it indicates that children and young people are becoming increasingly prone to such online harassment. Intermediaries have an important role to play in ensuring the cyber security of minors. For instance, Instagram has recently implemented a mechanism that will automatically make accounts of users under the age of 16 private to protect minors from online threats and risks.[13] Therefore, intermediary liability can be a very good tool to combat cybercrime.

4. Internet Intermediary Liabilities and Fundamental Right

Several international and national bodies have acknowledged the fundamental right nature of internet access, including the United Nations Human Rights Council[14], Costa Rican court[15] , and the Indian Supreme Court[16] declaring access to the internet as a fundamental right. Therefore, there is a concern of fundamental right in imposing intermediary liabilities. When it comes to the question of fundamental rights in imposing intermediary liability, apparently it seems that to some extent it imposes a bar on exercising the right to information and the right to freedom of expression. Popular opinion is that censorship of content is a violation of freedom of expression, and rendering electronic data inaccessible is a violation of the right to information, etc. However, a closer look shows a different scenario. The Preamble of the Right to Information Act, 2009 declares the right to information as an inalienable part of freedom of expression. Freedom of expression is guaranteed under article 39 of the constitution.[17] However, this right is subject to reasonable restrictions on the ground of security of the State, friendly relations with foreign states, public order, decency or morality, or concerning contempt

[10] Star Online Report, 'Noakhali gang rape: HC directs to remove video footage of incident from social media' *The Daily Star* (Dhaka,5 Octobor,2020) <https://www.thedailystar.net/noakhali-gang-rape-high-court-directs-remove-video-footage-incident-social-media-1972893> accessed 5 August 2021.

[11] UNB, '49% Bangladeshi school pupils face cyberbullying' *The Daily Star* (Dhaka, 2 February 2016) <https://www.thedailystar.net/bytes/'49-bangladeshi-school-pupils-face-cyberbullying'-287209> accessed 3 August 2021.

[12] Staff Correspondence, 'Children faced online harassment during the pandemic: ASK study' *The Daily Star* (Dhaka, 1st March 2021)<https://www.thedailystar.net/city/news/children-faced-online-harassment-during-the-pandemic-ask-study-2052877> accessed 3 August 2021.

[13] James Vincent, 'Instagram is making accounts for users under 16 private by default' (The Verge, 27 July 2021) <https://www.theverge.com/2021/7/27/22595897/instagram-under-16-accounts-private-default-limited-advertising> accessed 7 August 2021.

[14] UNHRC 'Report of the Human Rights Council on its twentieth session '(3 August 2012) UN Doc A/HRC/20/2 <https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session20/A-HRC-20-2_en.pdf> accessed 7 August 2021.

[15] Andres Guadamuz, 'Costa Rican court declares the Internet as a fundamental right' (TechnoLlama,2 October 2010) <https://www.technollama.co.uk/costa-rican-court-declares-the-internet-as-a-fundamental-right> accessed 15 September 2021.

[16] Staff Correspondence,'Access to internet is a fundamental right, says Supreme Court' Hindustan Times(New Delhi,11 January 2020) <https://www.hindustantimes.com/india-news/access-to-internet-is-a-fundamental-right-says-supreme-court/story-miomQARGJTy7Cz1WPazENI.html> accessed 15 September 2021.

[17] The Constitution of People's Republic of Bangladesh, art.39.

of court, defamation, or incitement to an offense.[18] According to article 19(3) of the International Covenant on Civil and Political Rights, restriction on freedom of expression can be given by law for respecting the rights or reputations of others, protection of national security or public order, or public health or morals.[19] Therefore, imposing intermediary liability falls under reasonable restriction since it is imposed for protecting the rights of others, of national security or public order, etc.

It is argued that the legality of the content in question should be determined by a separate impartial judicial body, and not by private intermediaries. This is not because intermediaries lack the necessary legal expertise in making such determinations, but rather because fundamental legal principle requires that actions affecting fundamental rights be applied by an independent court rather than by private bodies.[20] Counterpart argues that potentially harmful and illegal contents require immediate takedown. Waiting till sending the question to the said body will make the process lengthier and will not serve the purpose. For instance, a personal moment of someone got spread on social media, if the intermediaries wait till sending it to the judicial body, then it will start to spread more since, at present, one tap can make something viral in an hour. In reality, intermediaries are best qualified to block, filter, or remove unlawful content because intermediaries have the technical and financial resources to do so. Furthermore, as internet intermediaries earn profit from the propagation of content of third parties in their platform, they should share the responsibility for preventing access to unauthorized or detrimental material as well.

Another argument against the intermediary liabilities is that there is a possibility of misuse of the law by the government for political purposes. However, it can be argued that there is a judiciary that can anytime review the law. Nevertheless, a proportional balance and harmony are always necessary for imposing intermediary liability.

It is mentioned earlier that Intermediaries can develop AI features to censor offensive, obscene, and unlawful content. It is indeed true that it can undermine fundamental rights, since the system may be unable to distinguish between unlawful and lawful content adequately, which may result in the censorship of lawful content.[21] However, this dilemma can be overcome by further making it subjected to human judgment.

5. Diverse mechanism of Internet Intermediary Liability

Various experts have conceptualized diverse approaches for intermediary liability. In general, when legislation regulates intermediary liability, three models are considered.[22] These are defined by MacKinnon as strict liability, safe harbor or conditional liability, and broad immunity.[23] Under strict liability, an intermediary is responsible for any unauthorized third-party posting, although it is unaware of the illicit material.[24] Intermediaries can avoid responsibility by monitoring, applying restrictions, and removing allegedly unauthorized information.[25] In conditional liability, the intermediary gets a shield from liability if it meets

[18] ibid
[19] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR), art. 19 (3).
[20] Article 19 (n 5).
[21] Frosio (n 2).
[22] MacKinnon (n 3).
[23] ibid.
[24] ibid.
[25] ibid.

certain criteria, such as deleting inappropriate content after getting a complaint or alerting the provider of illegal content after receiving a notice.[26] And lastly, the intermediary is exempt from third-party information over the last model, known as broad immunity, irrespective of the unauthorized information.[27] Most of the countries follow the above-mentioned three models to regulate law for intermediary liability. In this paper, we have categorized different countries in three parts such as -Asia, The USA, and European countries and we have discussed how states around the world have coped with this matter-

Asia

In Asia, the majority of countries adhere to the strict liability and safe harbor approach. China and Thailand are two prominent countries that govern intermediary responsibility with strict liability. Intermediaries in China are deemed to be vicariously liable if their knowledge regarding unauthorized acts on their platforms is proved.[28] In Thailand, sections 14 and 15 of Computer-Related Offences Act B.E. 2550 (2007) deal with intermediary liability. Following these provisions, internet intermediaries will not get exemption from accountability on the ground that they did not commit the crime.[29] They will also be held liable for the act if it is committed within their platform or service.[30] When it comes to our neighboring nation, India, they adopt the safe harbor concept. In India section 79 of the Information Technology Act of 2000 grants conditional exemption to intermediaries who fulfill the required due diligence standards. [31]

EU- e-commerce directive

The e-Commerce Directive is the legal mechanism that underpins all internet platforms in the EU. EU-e-commerce directive also adopts the safe harbor model. To get shielded from liability network service providers or the internet, firms need to delete unlawful information or conduct from their services after being notified of its availability.[32] To make intermediaries liable, their actual knowledge is need to be proved.[33]

USA: Section 230 of Communications Decency Act

Unlike other countries, The USA follows a broad immunity model. Section 230 of the Communications Decency Act of 1996 grants exemption from responsibility for the conveyance of any third-party material to internet services, including intermediaries. It expressly specifies that suppliers of an "interactive computer service" would not be considered third-party content providers.[34] The clause also states that such internet services may review and erase harmful or indecent third-party contents in "good faith."[35]

6. Reflection on the Safe Harbor Model in Bangladesh

[26] ibid.
[27] ibid.
[28] Jie (Jeanne) Huang, 'Internet (Un)Immunity: Where Does China Stand?' (2020) 7(2) Asian Journal of Law and Society 345.
[29] Computer-Related Offences Act B.E. 2550 (2007), ss 14,15.
[30] ibid.
[31] The Information Technology Act 2000, ss 79.
[32] Directive 2000/31/EC of the European Parliament and of the Council of 17 July 2000 on certain legal aspects of information society services, in particular electronic com merce, in the Internal Market [2000] OJ L178/1, art 14.1.
[33] ibid.
[34] The Communications Decency Act of 1996, ss 230.
[35] ibid.

Bangladesh's intermediary liability framework flows from section 79 of the Information & Communication Technology Act, 2006 (hereinafter the ICT Act) and section 38 of the Digital Security Act, 2018 (hereinafter the DSA). Both these sections articulate the safe harbor model which is operating as a shield for the intermediaries. These clauses permit network service providers to deflect accountability for third-party content if certain requirements are met. The primary criterion that must be met is that the act or violation was undertaken without their insight or that they used reasonable effort to avoid the occurrence of such violation or infringement.

In short, actual knowledge will play the key role to hold internet intermediaries liable which is a reflection of the Safe Harbour Model.

7. Are the Existing Laws and Liabilities Sufficient?

In Bangladesh, section 79 of the Information & Communication Technology Act, 2006 and section 38 of the Digital Security Act deal with intermediary liability. However, these two laws do not define the intermediary properly. ICT Act only says that network service provider means an intermediary[36], and concerning the data message, an addressee[37] and an originator[38] do not include any intermediary. However, the Act is silent about the definition of intermediary concerning any particular electronic message. Section 79 of the ICT Act of Bangladesh is almost identical to section 79 of the Information Technology Act, 2000 of India. But they have defined intermediary concerning any particular electronic record[39]. ICT act defines intermediary in a generalized way and imposes equal liability and condition to all the intermediaries irrespective of their types. This will not do any better since each kind of intermediary has some distinctive features. In India the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 introduce two new categories of intermediaries: "social media intermediaries"[40](defined broadly) and "significant social media intermediaries"[41] (those with registered users above the 5 million thresholds) and additional obligations have been imposed against the second category of the intermediary. As Bangladesh follows the safe harbor principle, intermediaries are protected against liability for content posted by their users on their platforms. However, this protection applies only when intermediaries follow due diligence. But what sort of due diligence they have to follow has not been mentioned in the ICT Act and DSA. In India, as per the new rule of 2021, intermediaries have to exercise due diligence about three main things: (i) periodically informing users about rules and regulations, privacy policy, and terms and conditions for usage of its services, (ii) blocking access to unlawful information within 36 hours upon a Court or government order, (iii) Keeping records of removed information for 180 days for investigation, including deleted user profiles.[42]

It is indeed true that defining "due diligence" is close to impossible. However, some major and most necessary diligences should be mentioned in-laws like India's.

---

[36] The Information and Communication Technology Act 2006, ss 79.
[37] ibid, ss 2(21).
[38] ibid, ss 2(23).
[39] The Information Technology Act 2000, 2(1)(w).
[40] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, ss 2(1)(v).
[41] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, ss 2(1)(w).
[42] Diganth Raj Sehgal, 'Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021' (IPLEADERS, 14 July 2021)<https://blog.ipleaders.in/information-technology-guidelines-intermediaries-digital-media-ethics-code-rules-2021/> accessed 7 August 2021.

At present, some intermediaries can implement AI features to censor offensive, obscene, and unlawful content. However, they are not implementing the AI feature and adequate defensive measures since it will result in loss of revenue or traffic. As a result, it is reasonable to state that the current legislation is inadequate.

8. Recommendation

From the above-mentioned analysis, it be can be said that existing laws should be amended and a new set of rules should be introduced regarding intermediary liability to prevent future complexities. The amended law should include the following things-

Incorporation of internet intermediary terminology in the border sense:

As previously stated, existing laws provide a generic definition for the phrase intermediary liability. There is no mention of culpability for internet intermediaries. Here, Bangladesh can consider the European Union's Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 and the EU e-Commerce Directive regarding the definition of internet intermediaries.[43] In the definition, the following delegate criteria should be included:

- Network service provider,[44]
- Internet service provider,[45]
- Website hosting companies,[46]
- Social media platform,[47]
- Search engine operators.[48]

Every one of these service providers, social media platforms, and companies will come under the category of internet intermediaries.

Implementation of the notice-to-down and notice-to-notice procedures for monitoring unauthorized content:

The "Notice and takedown" technique includes intermediaries depleting substance that is prohibited by law as soon as they become aware of it.[49] And in "Notice and notice" method compels intermediaries to alert the originator of illicit substance before moving ahead with any action. Both of these methods must be enshrined in law.[50] "Notice and takedown" must be implemented for any heinous offense including child pornography or sexual material. Notice and notice methods should be followed for petty cybercrime.

Responsibilities regarding criminal proceedings:

---

[43] Directive 2000/31/EC of the European Parliament and of the Council of 17 July 2000 on certain legal aspects of information society services, in particular electronic com merce, in the Internal Market [2000] OJ L178/1.
[44] The Information Technology Act 2000, 2(1)(w).
[45] Association for Progressive Communication, 'Frequently asked questions on internet intermediary liability' (APC, 19th May 2014) <https://www.apc.org/en/pubs/apc's-frequently-asked-questions-internet-intermed> accessed 16 September,2021.
[46] E-Commerce Directive, art.14.2.
[47] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, ss 2(1)(v) and ss 2 (1) (w).
[48] *Google France SARL and Google Inc. v Louis Vuitton Malletier SA* (C-236/08).
[49] ARTICLE 19, 'Internet Intermediaries: Dilemma of Liability Q and A' (ARTICLE 19, 29 August 2013) <https://www.article19.org/resources/internet-intermediaries-dilemma-liability-q/> accessed 16 September, 2021.
[50] ibid.

According to the Hungarian Code of Criminal Procedure, any public body, commercial organization, or public organization can be asked to provide or transmit information.[51] As a result, when intermediate service providers and other online communications service providers get such a request, they must disclose the requested data to the asking entity.[52] Here, Bangladesh can consider this model and include it in existing laws that when internet service providers are asked to disclose data to help the criminal proceeding, they will have to do it.

Categorizing intermediaries in a different group based on their user base:
Equal liability in every case for all intermediaries will in itself create an inequality since they have different user bases. The intermediary who has 20 million users and the intermediary who has 2 million users should not be imposed with equal liability in every case, since intermediaries with small numbers of users do not earn similar revenue. Therefore, intermediaries should be categorized considering their number of users and additional obligations should be imposed on the intermediaries who have more users.

Fulfilling the requirements of the laws of Bangladesh:
Adequate legislation would establish a level playing field among all internet intermediaries by requiring all intermediaries to meet certain minimum security and defensive measures. At present, policies, terms of service, and user agreements of intermediaries do not meet the requirements of laws of Bangladesh since they are not bound to. Rules should be introduced to make the intermediaries bound to include content regulations and other requirements of municipal laws of Bangladesh into their policies, terms of service, and user agreements.

9. Conclusion
Whereas sections 79 of the ICT Act and 38 of the DSA explicitly state the limit to which an intermediary is accountable, one gap appears that the definition of intermediary is constrained to network service providers solely. The online world is blooming. Nonetheless, the number of wrongs committed through the internet expands every year. Cybercrime is on the upswing as a consequence of the lack of comprehensive guidance on internet intermediary liability. When internet intermediaries have the potential to combat cybercrime, they should be urged to do so through a specific legal framework. To sum up, a liability system is needed for Internet intermediaries to keep working in compliance with their general concept of free expression and can also be held accountable for unauthorized content to combat cybercrime.

[51] The Act No XC of 2017 on Criminal Proceedings, ss 261(1).
[52] ibid.