DISSERTATION

ON

Liability of Internet Service Providers: Safeguard of Personal Data.

Course Title: Supervised Dissertation

Course Code: LAW 406

Submitted to:

Sayeed Hossain Sarwar

Lecturer, Department of Law

East West University

Submitted by:

Anika Tasnim

ID: 2017-1-66-021

Date of Submission:

7.09.2022

Word Count:

6680

(Excluding Footnotes)

A thesis submitted in conformity with the requirements for the degree of Bachelor of Laws, Department of Law, East West University.

Acknowledgement

It is my honour to express my deep and sincere gratitude to the honourable Assistant Professor and Chairperson, Department of Law, East West University, Dr. Mehedi Hasan sir, for giving me such an opportunity to do this thesis work. I am also very grateful to my Supervisor, Sayeed Hossain Sarwar, the Lecturer, of the Department of Law, East West University. He helped me unconditionally to choose this topic. He also helped me to organise the chapters, the taught me the methodology to carry out the research with professional touch and provided me invaluable guidance throughout the whole process from start to finish. This thesis would have been impossible without his help and unconditional support. I am also grateful to everyone who helped me willingly out with their abilities and lot of respect to everybody who are involved in this process.

Declaration

This is Anika Tasnim, I hereby declare that the submitted dissertation entitled **"Liability of Internet Service Providers: Safeguard of Personal Data"** is an original piece of work. To the best of my knowledge, I further declared that this dissertation has not been formed or submitted in any previous application for a degree. I confirm that the thesis is formed and presented by me only for the undergraduate program as **Law- 406 (Supervised Dissertation)** of the Department of Law, East West University. Any literature date or work done by others are cited within this dissertation has given due acknowledgement and listed in the footnote section. I also declared that this whole work is done by me with the professional guidance of my honourable supervisor.

Abstract

Internet service providers can easily get access to our personal data. The dissertation deals with the legitimate framework adequate to ISPs governing platforms for user-generated contents which is also known as user created contents such as images, videos, audios, texts which has been posted by the users in social platform. We can consider ISP as mere host provider who works with not only the allocation of data content, but also tagging and actions correlating to promotions of data in their websites. These actions often concerns third parties with privacy litigations. This dissertation will determine whether ISP is accountable in case of protection of information or not. This dissertation will also determine how the immunities work in favour of ISP in case of violation of privacy even when the data is being uploaded by users and it harms their right to privacy. The dissertation will deal with this topic through contiguous examination of facts, cases laws, judgement of the Courts along with the laws of some other countries, in particular USA, Australia, Canada, China and Europe."

List of Abbreviation

ISP: Internet Service Providers.

DSA: Digital Security Act, 2018.

ICTA: Information and Communication Technology Act, 2006.

Table of Content

Introduction:

In the era of 2022 most content accessible online is user generated. Every person who live together in a society they contribute to each other and that contribution create a growth of a universal strategy. If we calculate the process of contribution we can find out that is our social life is reshaping in every facet of mortal relationships.[1] The contribution made by human these days are mostly done through internet. Buying things, donations, ordering foods, expressing our emotions towards people everything is digitalise. The safeguard of our digital life must be keep in concern. Digital security includes illegal access to our data and information. As citizens of Digital Bangladesh people are getting more muddled with data available about their location and activities, the right to privacy seems to dry up. The new implementation is essential for a well-developed country in which we would wish to live. We know that Internet service providers provide internet connections and services to both individuals and organisations. It can be presumed that they might have some invisible power to know every detail of an individual's private life and they might be immune from legal liabilities in Bangladesh. The user generated content is not always socially beneficial and such thing is not very favoured. Sometimes it become necessary to remove the content. The content might contain "slander, crime, provocation to despise, child pornography etc." It may create an amount of legal problems. All these problems have been greatly examined in the books in recent years. This is very unfortunate that most of them are produced by the users. In this dissertation the details will not be measured out about whether ISP should be liable for negligence, rather, the aim is to discuss the recent trend of judgements about the "right to privacy" of users and the right to immunity of the internet service providers. Nonetheless, over the policy grounds it is not an easy job defend such immunity. Some tort law principles are also pointedly inconsistent with this facts because the service providers monitor the door through which way the internet disturbance enters to the public web.

[1] Neil Selwyn, 'The digital native myth and reality' (5 July, 2009), AP 61, 4 Emerald Publishing <https://citeserx.ist.psu.edu/viewdoc/download=10.1.1.156.2794&rep=rep=0.1&type=pdf> accessed on 19.6.22.

Methodology:

Theoretical or descriptive research are been made in the dissertation. The facts are mostly relies on relevant theories, provisions and different opinions of some scholars. In this study, the perspective of own hypothesis is being added. There are also some existing laws regarding this issue. In this paper the most used source is secondary sources. This research is primarily formed on the sources which includes statutes, case laws and as other sources includes online journals, websites, online articles, news reports and blogs from the internet.

Limitations:

Like all other research, this research does have some limitations. There is a confliction between the rights to keep our personal data privileged with other rights for example the right to collect information for business purpose. Internet service providers can access our information anytime though it will help us in some particular circumstances. Having access to user's information can help police to find criminals and this will reduce cyberbullying and other crimes related to the internet. We can see the benefit of free use of internet but online privacy is not absolute in this case.

Research Questions:

The primary question is

- What is the degree of protection of our personal data against the access of internet service providers on that?

The secondary questions are,

- How ISPs deal with people's personal data?
- Should ISPs be reading those data?
- Is ISP violating Data Protection rights of the consumers?
- What are the liabilities of an ISP for protecting people's personal data?
- What are the provisions in Bangladesh regarding this issue?
- What are the lacuna in the Bangladesh legal system regarding this issue?

CHAPTER II

Internet Service Providers (ISP) and User rights.

2.1 Who is ISP?

ISP delivers internet services to numerous people in our society. Along with codifying entries to the internet, software bundles can also be delivered by them. The bundles are presented as browsers, electronic mail accounts, and a personal forum like web sites, for example Google, Yahoo can be recognise as ISP. Websites for businesses can also be built by them. Through numerous entry points over the internet they all are connected to each other. By the growth of retail Internet services and dressings helps fuelling an immediate commercialization of the Internet. This manifestation is the outcome of several other components as well. Nonetheless, a maximum of these ISPs delivered only limited service and depends on accessing to regional and national ISPs for broader connectivity. Everything which have been executed by us over the internet can be detect by them very easily. They can learn very easily about which forum we are visiting or which device we are using including our location. Relying on our location in the world, for variety of goals, our data can be borrowed by our assembled profiles and can be sold to other party without our knowledge.[2]

2.2 Why dose ISP track customer's data?

We can presume that data regarding our internet traffic are being craved by the service providers in order to give us more service. It also makes them eligible to watch everything done by us online. However the case is not always like this way.[3] There is a reason behind ISP's desire to watch our browsing record. Well, there are some unusual possible explanations. In some states, compulsory data retention statutes prescribe that ISP in some special occasions can chase and document particular data which they can lawfully store of their customers. This might include the forum we visit, our electronic mails, watch and search history and the system we are using for this operations and among many other aspects. Our data can be utilized for

[2] Jim Harper,' Against ISP Liability' (2005) 28, Telecommunications and Technology, <https://heinonline.org/hein.journals/rcatorbg28&div=9.&id=&page=> accessed on 19.6.22.

[3] Doug Litchmen and Eric Posner, 'Holding Internet Service Providers Accountable' (2006), (Sup. Ct. Econ. Rev. 14, 221.), by University of Chicago <https://heinonline.org/hein.journals/supeco14&div=10&id=&page=> accessed on 22.6.22.

numerous reasons, but it is asserted by the government that it can only be done as per the conditions of law enforcement authority. And the act must be done for certain reasons which might be an anti-terror initiative.[4] If any corporation can found our browsing data or anything related to our life every details can easily be figured out by any skilled person. The data can be about the details of our bank account, what we buy and eat, and more private data like our matrimonial status, fitness problems and even sexual choices we can see no existence of privacy here. Just because data is correlating to dollars, ISP bargains for business and money with the advertisers and obtain data on behalf. Then we are targeted by the corporations with related advertisements on the web pages we visit. This would get more upsetting when our kids are being targeted. Our online family purchasing opinions are impacted by kids most of the times and these data can be very helpful to the marketers. VPN is used by many people. By using this people of many states can easily visit to the unrestricted we site, where there might be an enormous number of people who cannot. ISP can also learn information by stealing these data if they want to. Some entries are prohibited by the government to specific web pages for several reasons. For example the government can restrict the sites where can be part of hatred which may contain ill word or motivates actions that are against a specific theology including illegal site like porn or gambling. Particular states or areas could be obstructed from this. In this cases ISP is employed by the government to execute this censorship. Since, ISP have the right to access what sites we are exploring and it is them who award us with entry permission to those sites, they have the supervision to prevent entry as required by the government.[5]

2.3 What kinds of information is ISP tracking?

We know that every day some of our data is being tracked by ISP. What data is being gathered may differ between the providers of different areas. As the law relating to data retention differs from area to area, by learning about how and our which activity is chased may also rely on our territory. ISP's terms of service and privacy policy may have the details about conservation of data if anyone want to discover by any reasonable direction. Ambiguous and complicated wording might be used so the full length of the search can be tough. We should also be eligible to discover if the data may be distributed to other party. However it is presumed that this is

[4] Ibid

[5] Ni Ketut Supasti, Deris Stiawan 'Personal data protection and liability of internet service provider: a comparative approach', (2017), Vol 9, No 4, pp 3179-3184 International Journal of Electrical & Computer Engineering.

nearly could be the case. Get into the details about how data is used or shared without the help of skilled authority can be tough too.[6]

In USA a children's television station was been inhabited by the defendant service provider. They gave the kids some videos and interactive games by their forum so the children can enjoy their time. The condition for creating an account the user had to select a username and password. The kid had to deliver his or her information for example birthdate and gender to the provider during the enrolment procedure.it was clearly mentioned in the forum that, "HEY GROWN-UPS: We don't collect ANY personal information about your kids. Which means we couldn't share it even if we wanted to!"[7] It was alleged that the service providers learned and stored the data about the users and also accessed their web browsing history and when a user visited one of their websites, first-party cookie on that user's computer were set by them. An agreement was set between GOOGLE and the defendant. Google had the permission to publish their advertisements on the defendant websites. As a result, when an individual visits their website Google got an access to put third-party cookies on the computers including kids.[8] The complainants also asserted that, google could chase any user of that site and follow them in any forum once the cookie was being placed on the person's computer. And after that Google displays ads as per their wish.[9]

Their lawsuit was been declined by the court. Because google did not played with protected data as per the Act authorized. The charges brought by the complainant are only elements that reveal protected data and it was declared to be mere recipients of it. District Court's judgement in favour of the complainants' was totally an assertion for intrusion upon privacy. By this case Google learned a lesson that such a lawsuit might bring trouble to them because they vowed to honour customer privacy and then violated their own obligation. It was sufficiently asserted by the complainants that the private data was been obtained about users despite its promise not to do so, and an adequate jury might assume that such action was highly offensive under law.

---

[6] Ibid

[7] *NICKELODEON CONSUMER PRIVACY LITIGATION [2016]*, No 00 15-14 41, 827 f.3.D 262 United States Court of Appeals, Third Circuit.

[8] Ibid

[9] Ibid

2.4 Privacy rights of the Customers:

Online privacy of the customers arises when the information we do not want to share are being ranged from the information we provide on purpose. There are so many questions regarding the rights of ISPs be reading our bits.[10] It was argued in an article about under-burdened privacy and liability of the providers, they confirmed that they will follow the law. As per the law their delivered data will not be surveyed or duplicated or stored or dealt against essentiality to deliver good service. ISP has a business model and according to that model that they have the right to examine user data and in some cases exchanges of user data provides moderately less fees.[11] The similar structure of data is carries by ISP and telephone companies. The transmitting equipment of ISP is mostly in digital form, which is not very tough to assemble, portrait, and analyse. The ISP context is more risky regarding privacy and safety. On the other hand the requirement of telephone service is less deep. Being an entry provider if ISP cannot enjoy the right to copy or comprehend the transported data than the phone companies also have no right to listen in-on calls or the postal service must not look for the mail it provides. It was suggested that, the ISP must do a survey for customers' extra ordinary symptoms and examine their behaviours to be accountable and possibly protect user's data sources for a specific amount of time. [12] These statements are hectic debates right now. It became a goal to compel ISP to conserve data of the customers from the data sources. European law enforcement councils did not want to give up on the recommendations for their goals.

The contents of email exist in ISP's network. What a state or police cannot do internet service providers can.[13] ISP can legally saw some conversations of us and third parties we engaged in. their rights to search email contents are not limited.

[10] Jim Harper,' Against ISP Liability' (2005) 28, Telecommunications and Technology, <https://heinonline.org/hein.journals/rcatorbg28mdimv=9hid=&page=> accessed on 27.6.22.
[11] Ibid
[12] Jose I. Rojas, 'Liability of ISPs' (1998), 507 PLI/Pat. 1009, 1016-17 Content Providers and End-Users on the Internet.
[13] Steven R. Morrison, 'What the Cops Can't Do, Internet Providers Can: Preserving Privacy in Email Contents' (2011) Vol 16 Va. JL & Tech, University of Virginia.

CHAPTER III

ISP liabilities in different countries:

The problem of whether Internet Service Providers should be responsible for having access to data that ascertains injurious to others has attained enough attention in the previous argument that the normative statements for various reasonable liability regimes have been substantially conveyed. Surely, courts can barely announce upon the effect one direction or another without being condemned.[14] Several acronyms are used to illustrate Internet Service Providers and related businesses.

1. USA

In most of the cases ISP had been held secondarily accountable in United States. In USA one have to be a qualified service providers to attain local liability under the stable harbours. The expectation of the essential rules of accountability must be keep in mind. The adoption of sufficient execution of infringer method must be adopted. This methods must include an example of sufficient conditions between users and the service provider.[15] Yet, some modified technical measures must be taken by the ISP. This must be made in their standard forms. This forms will be used by the holders of copyright to identify or protect their works.[16] It also be fulfilled through the requirements of a private stable harbour by the ISP. It need to be fulfilled under the conditions of comfortable harbour as per section 512(c). This section covers the statements regarding infringement that occur by the repository path of a user appliance. It also occupies on a network governed by the ISP. A considerable awareness must have to be provided by the ISP that the object and the activity occurred by using the device on the policy is infringing the validities which is violating the action is apparel. The mastery or reasoning must respect "specific infringing activity."[17] Under American Law, ISPs have a regime known as the Notice and Takedown regime where they are compelled to kill violating posts through a

[14] *Doe One v. Oliver*, [2000], A. 0755. 02d 1000 (Conn. Ct. Super. 2000*); Lunney v. Prodigy Servs,* 723 NE 2d 539 [NY 1999].
[15] ibid

[16] VK Unni, 'Internet service provider's liability for copyright infringement-How to clear the misty Indian perspective' (2001), Vol 8(2) 13 Richmond Journal of Law & Technology.

[17] ibid

formal way. [18] ISP like YouTube enforced an equipment in recent days. This equipment detects copyrighted topic when there is a overstepping process in recognised. This automatically remove the copyright part.

2. Canada

ISP is held secondarily liable in Canada. Liability of ISP characterised as an abrupt violation in this country. In 2012 to The Copyright Act was modified. A modern kind of detriment was prescribed by this modification. This modification encompassed some stable shelters through a report and notice regime. By this modification copyright infringement was bring into light over the Internet. Stable harbours are acceptable to ISPs, catching services, storage service and search engine providers.[19] In Canada a compulsory obligation was not taken out by the ISPs regarding the violating topic. They improved their position day by day. However daily filtering duties was not properly compelled by the Canadian law.[20]

3. Australia

As per the doctrine of authorization ISP also held secondarily responsible in this country.[21] A deduction of a section 112E was made from Australian Copyright Act. Deduction of this section gifted ISP with some special safe harbours. Four stable harbours was provided in the copyright act of Australia. Section 166AA provided the list of action that are associate to the violations. They are correlated with conducting certain online actions. Section 116AC46, Section 116AD47, Section 116AE48, and Section 116AF49 infers the four trends of safe harbour. Section 116AH50 stated that the general restrictions must be fulfilled by the service providers. Some special and detailed situations were being listed for the known stable harbour sector. Australia would not evaluate a beneficial stance to ISPs respecting the deterrence.

4. China

---

[18] *Fonovise V Cherry Auction*, [1996], 76 F3d 259 [9th Cir].

[19] Pamela Samuelson, 'Regulating technology through copyright law: a comparative perspective' (17 July, 2020), Vol 3. 72(2) European Intellectual Property Review, University of California, <papers.ssrn.coM> accessed on 7.8.22.

[20] ibid

[21] *Goldberg V Lee Express Club Corp*, [1995] 634 NYS2d 337.

On fault based laws ISPs were held secondarily liable in China. Most of the cases are in relation to the principle of negligence or principle of joint or accessory of penalty. For being held liable the defendant must have to have the knowledge of a contributory infraction either for joint or accessory liability. And the defendant have to have actual knowledge of the offense. In 2006 the regulations were enacted. Some stable harbours were been delivered by the regulation to ISP. The variation of network that made the service providers eligible for safe harbour were being demonstrated by the law. It also described the part when they are not favourable.[22] Eventually it must be defined that no rule fending off the imposition against copyright violation that can examine obligation under the Provisions passed in 2013 had been enacted by China.

Most popular feature of Google is the auto-fill button. It helps the users by providing the information and filling the appropriate fields in a web form that they had already put in another website.[23] This survey stated that 61% of respondents would like to have the same feature where 51% of respondents said that they would like to have a similar feature which will fill out the forms automatically only for the sites that have the similar privacy policy as the one where the users previously provided their information. On the other hand, 39% of respondents express their willingness in such a feature where it would automatically send the information to the website while they visit that site again. So, a feature of an automatic sending of data to the web site was created. Some respondents showed interest in these features because everything was organized without any intervention of the users. Among these, 14% of respondents are interested in the feature that would notify the users that it had sent the information and another 6% respondents are interested in the feature that would not notify about the transference of the information to other websites. [24]However, 86% respondents of that survey did not show any interest in such a feature where it would transfer the information without any intervention of the user. The findings of their survey are also consistent with other surveys on the account of the user's priority to privacy over convenience, such as the GVU survey, held in 1998, respondents in amount of 78% stated that they are concerned about privacy more. These data from the surveys clarified that the privacy issue plays a role over the technical features.[25]

---

[22] ibid

[23] Lorrrie Faith Cranor, Raeagle Joseph, Mark Ackerrman, 'Beyond Concern: Understanding net user's attitudes about online privacy' (2000), Vol 47-70 The Internet Upheaval: raising questions and seeking answers, <arxiv.org> accessed on 5.8.22.

[24] Benassi, Paola, 'TRUSTe: an online privacy seal programe' (1999), 42(2), 56-59 Communication of the ACM,. <dl.acm.org> accessed on 8.8.22.

[25] Culnan, Maryn J, 'HOW DID THEY GET MY NAME?' (1993), 17: 341-364 MIS Quarterly <https://www.jstor.org/stable/249775> accessed on 9.8.2022.

The findings of the survey states that the respondents are highly concerned about their privacy and they provided strong opinions about automatic transfer of information. Among them, a large number of respondents gave the opinion that they want to be in control of the processing and usages of their data and they do not want to transfer their data automatically. Though some respondents express their intention to provide data automatically but maximum number of respondents want to have control over their information.[26] Sometimes the website may look similar but their privacy policy may not be the same. So, it is convenient for the users if they have the control over their information and have the complete right to share their information to the website on their own.

5. European Union:

In case of the violation of data protection and the matter of accountability of ISP regarding this matter has also been arisen in many EU member states. The government have taken various methods on this matter. In this dissertation two cases will be cited as proof of the pervasiveness of this matter. In Google v Vividown[27] three executives of a famous company like Google were found guilty because they violated the data protection law. They uploaded a video about a disabled individual being taunted and humiliated. The judge added that the video was being processed without putting up with sufficient preventive criteria and it did not avoid privacy violations. It also did not adequately notify the particular engaged users to perform their responsibility where they were not allow to post personal data which is assembled as illegal and the criminal conviction was knocked down. Nothing was brought in front of the court regarding the ISP's exemption from liability not even detailed references. The learned judge might believe that exemption regarding ISP violation of law did not coat under data protection. A literal variation can be found if the "Article 1.2" of the Italian Legislative Decree on e-commerce. Spain included a safe harbor article without mentioning the National Data Protection Authority[28]. It listed who would be liable for data protection violations. The law was enforced by article 16 of Law 34/2002 of the e-Commerce Directive. It asserted that not but the users would be held accountable for violation of data protection directive. In European

[26] Ibid.
[27] Natalia E. Curto, 'EU directive in copyright in the digital market: what next at in international level? ' (2019), vol 11 no 3 Journal of law technology and internet.
<https://heinonline.org/bandle=hein.journals/caswestres11&div=5&id> accessed on 10.8.2022.
[28] ibid

countries it is appeared that as per the article 14 of the directive the ISP liability issue revolved around the term “hosting services”. Which most typically contended as a confronted issue before the courts. It was recognized that commonly the court required to find out the position of the accused ISP. It was necessary to find that whether the ISP qualified as a hosting service or not. If it is found as a hosting service then could they being excused from liability regarding violation of copyright law.

In June 2007, French humorist Jean-Yves L successfully filed a suit against MySpace.[29]Several designs of the author had been displayed by the users on a forum. Which was clearly an infringement of the author’s right. In this case the statement of the defendant was denied by the High Court of First Instance. The defendant argued that they were not liable Article 14 because they were delivering a “hosting service” authorizing safe harbor. The court clarified that MySpace should be classified as a “publisher”. The reason behind this was the defendant had skilled members who were authorized to build personal Web pages within a specified frame system. A good portion of revenue was being collected from their advertisements. So the court held that the defendant party cannot enjoy the exemption under Article 14 of the E-commerce Directive. They was found instantly liable. For the purpose of enforcing IP rights, it was imposed by the French court that a significant amount of care must be taken regarding the data protection rules on ISPs[30]. In this issue, there was a case filed by a film company against Google for unauthorized streaming of their film "Tranquility Bay" on their website.[31] Even though Google removed that video from its website every time it got a takedown request, users kept reposting the movie there. Following the definition provided under the E-commerce Directive Article 14, it was decided by the court that Google met the requirements to be considered a "hosting service". To enforce IP rights it was shown that they had done enough, the court stated that for copyright infringement Google was partly at fault and it also held that after all of these google had a duty to take every necessary step to stop their further publication. Finally, Google was found to be responsible by the court due to its failure to follow the requirements provided under “Article 6-I-2” in respect of each and every upload.

[29] Seagull Haiyan, ‘Comparative copyright analysis of ISP liability in china versus USA and Europe’ (2010), Vol 27 no 7 the computer and internet lawyer. <https://papers.ssrn.com/sol3.kjg/papers.cfm.id.okiu.=2118961> accessed on 5.7.22.

[30] Edward Lee, ‘Decoding the DMCA safe harbor’ (2009) 233, 32 Colum JL and Arts. <https://heinonline.org/hein.journals/cj.jhyj.098.la32&div=18&id=&98hhpage=> accessed on 1.7.22.

[31] ibid

In *SABAM v. Scarlet*,[32] the complainant filed a case against Belgian Web site Scarlet for knowingly allowing unauthorized downloads of SABAM's copyrighted content via P2P file sharing on their website. Scarlet was ordered by the Brussels Court of First Instance to implement the content management and identification system based on fingerprints. The court also urged Scarlet to take more effective measures to prevent its users from sharing copyrighted content without authorization. Cases similar to these following type could be found in Sweden (Pirate Bay, 2009) and Germany. In those cases the hosting characters of ISP can be recognized by the court however it was found that the ISP was held liable for the infringement of publishing copyrighted materials due to their failure because not connecting with the requirements provided under the Article 14 of the Directive. So it can be said that the ISPs have to follow the requirements provided under the Directive to avoid such allegations.

CHAPTER IV

Privacy law regarding ISP in Bangladesh.

4.1 Law of Bangladesh:

The privacy of the citizens is protected by the Constitution of Bangladesh and the DSA. Both are specifically concerned with right to privacy of citizens through real life and social media. It was provided in our constitution Art43 that the rights subject to any reasonable grounds imposed by the law in respect to their privacy is enjoyable by every citizen. The term 'personal information' is specified in section 26 of DSA and the section also furnishes that the term 'identification of information' shall include any data concerning our identity which is easy to access and function through technology. It is assembled by this section that storing and processing of "identification information" without having the legal authority and collecting such data, a person shall be held accountable and the punishment is imprisonment up to “five years or fine up to five hundred thousand taka or both for the first time offence”, and for the following to similar offence he will be accountable for imprisonment up to "seven years or fine

[32] ibid

up to ten hundred thousand taka or both" Privacy is also a fundamental human right that is acknowledged by the UN Declaration of Human rights.

4.2 Lacuna in the law:

In Bangladesh the immunity of internet service providers from their liabilities is in extreme. Bangladesh have the DSA that illegalize a number of cybercrimes, containing illegal reaching data infrastructure; unlawful access to computers or networks;[33] destroying or alternating of computer source code used on computer programs, systems or networks;[34] digital or electronic forgery and fraud;[35] identity fraud;[36] cyber terrorism;[37] and hacking.[38] In case of ISP section 38 of DSA provides that if a service provider try to access to any data information and proves that the offence or breach was committed due to unwillingness shall not be liable under this Act. This section gives the right to free access to our data which is contradictory to our right to privacy. In other countries ISP secondarily held liable in most cases. Bangladesh have almost zero cases regarding ISP's privacy violation or about selling our data to others. In most of the cases users are unaware or irresponsible regarding the matter that their data is being tracked by ISP which is harming their right to privacy. Section 30 of ICTA, 2006 provides that without prejudice to the section 45 a controller or any person authorised by him with a reasonable cause like investigation purpose etc. can collect or access to the system of machinery to get the related material and the person so directed shall be bound to extend co-operation in accordance with such direction.

---

[33] Anayna Azad, 'Digital security Act in Bangladesh: The Death of Dissent and of Freedom of Expression' (2011), vol 7 pp 732 Central European University. <https://www.coursehero.com/file/116871592/azad-ananyapdf/> accessed on 3.7.22.

[34] ibid

[35] Ibid

[36] Benjamin, Litchmen and Howard, 'Telecommunication law and policies' (2001) vol 32 Carolina Acad Press. <https://papers.ssrn.com/suol03/abstract_id=278698> accessed on 2.7.22.

[37] *Zeran V America Online* [1997], 129 F3d 327 [4th Cir]

[38] *Grace V Ebay, Inc.* [2004] WL 2376664.

CHAPTER V

Recommendation and Conclusion:

5.1 Recommendation:

From the legal viewpoint, Bangladesh is living by the rules of administrative perspective. It is very necessary to shift to civil perspective from this position.[39] The secondary liability theories fulfilled their task lawfully. Similarly, the velocity of settling the cases regarding enforcement need to be improved. To stop the crime a quick reaction is needed from the user from enforcement councils, therefore, the official websites can be notified without any interruption and receive the response[40]. However, to prevent misleading reports it is significant that users are made to provide sufficient evidence of the crime. This approved method is used internationally also by YouTube and Facebook. A rigorous level of penalty is required into the law that need to be as same as to hold ISP accountable is unnecessarily depended on immediate liability theory. We can see that there are so many list of circumstances in which ISPs may be liable but instead of doing this the law must provide safe harbors for ISPs whose damage caused to the right-holders. For participating in the movement against IP infringements the service providers are also liable.[41] There are strong arguments about how come the liabilities can be imposed to the Internet service providers for their violation of rights. Individual who is doing bad activities in internet is very difficult to identify. Internet pests or worms are routinely programmed by the ISP to catch them.[42] So the normal people usually fall for the traps. The law could order ISP to record and protect their service with lawful authority with court's order in hand so only lawful officials could get those information from them and use them for lawful

---

[39] Jenifer Arlien, 'The Potentiality Perverse Effects of Corporate Criminal Liability' (1994), 833 J Legal Stud, 833 <https://www.journals.uchicago.edu/duoi/0010.1086/467947> accessed on 4.7.22.

[40] Ibid

[41] *Chubby Inc V CompuServe, Inc*, [1991] 776 F Sup. 00135, 00139-0040 [SD NY].

[42] Eric Luenieng and Waaylie Wong, 'Virus Set for Jan 1' (2001), 23.4.2001 CNET News.

purposes. The role of the ISP can be defined through numerous ways.[43] Co-accountability seem to be found in ISP in case of the breach of privacy. An amount of norms are provided by them through which the execution of privacy infringement is being made and it is also done for the profit. Also, for the improvement of illegal circulation ISP make data easily available and searchable. They furnishes a similar uncensored program which is free for the users which they intend to do for personal gain. Sometimes they do it to the free growth of inhabitant's character and to become part of the social and political controversy.[44] Whether or not ISP should be held accountable and in what instance they should held liable depends on the criminal user generated topic which may describe the multifaceted role of ISPs. And the various legal significance pertained to their activity, clarifies why there is an on-going discussion. Two situations are expected for the ISP for their own safety. First of all, the accomplishment of a distinct activity by the users must be in consciousness of the internet service provider, and secondly, the provider must be aware by the content generated data which can infringe someone else's rights. While deeming whether to restrict the liability of ISP the first facet must often been remembered. On the other hand since the provider cannot not relatively control all user generated content the provider cannot be made accountable. Nonetheless, we must take into consideration of the second facet also. We also must think while taking ISP responsible for illegal activity that we need a skilled authority to find out if the content is illegal or not rendering illegal content hosted in its outlet. Thus the careful behavior of the provider is must in this cases to prevent feasible liability, in the cases where can be found a minor risk of a judicial decision in favor of privacy this would satisfy censorship, the freedom of expression can be found in extreme restriction in this cases.[45] If someone wants to prevent the distribution of data about themselves a hazard can be found in this cases because this will endanger the ISP in privacy violation litigations and by cleansing the fearful content the providers can be provoked even when the legitimate critique is conveyed.

5.2 Conclusion:

ISP has the freedom to influence people's creativity which can also endangered the safety protocol. This must not be withheld that ISPs play a decisive part in the recent period of

[43] Rab, D Charles and Collin J, 'THE DISTRIBUTION OF PRIVACY RISKS: WHO NEEDS PROTECTION?' (1998) Vol 14(4), the Information Society. < https://www.tandfonline.com/duio/abs/1080.1080/019722498128719> accessed on 19.8.22.

[44] Ibid

[45] Ibid

time.[46] They have been found accountable in many jurisdiction under both immediate and indirect liability theories. In order to harmonize with the worldwide norm and to protect the online life Bangladesh legislation need some changes. If the provision of DSA is been directly violated by ISP while being held accountable for free will then it is essential and viable to hold them liable for infringement through online activity.[47] The present phase of Bangladesh is to raise people's awareness over online safety is given less importance than the protection of users. Nonetheless, for monitoring the content Bangladesh legal system should need to adopt contemplate general obligation in order put a safeguard of the capability to technology development as well as a level of specialized investigation at the time. It also pertains to the ISP, on whose forum the content is released and allocated. The questions is the data controller is the provider or what if the user himself is the provider. In what circumstance the distribution of online activity can be deemed to be a private and which data safety protocol is inapplicable and what is applicable while having restricted accessibility. There is also a question whether the violation of privacy interested because of the exemption penalty for host in different circumstance.[48] It was seemed that the recent regulations regarding data protections limiting the liability of ISP regarding user-generated content provide the balance between most reasonable interests and the involvement of rights. There is nothing excluded in this finding regarding the necessity for taking initiatives in the schooling of the customers with concern to the safeguard of personal data.[49]

[46] Ibid

[47] Ibid

[48] Ackerman, Mark S. and Lorrie Cranor, 'Privacy critics: UI Components to Safeguards Users' (1999), Vol 2. 15 CHI EA'99: CHI'99 Extended Abstract on Human Factors in Computing Systems. <https://dl.acm.org/dnd/vgd/10.1145/6jd4889.74688> accessed on 22.8.22.

[49] Ibid

Bibliography:

Books:

1. Graeme B. Din Woodie, Secondary liability of ISP (2017)
2. Addams Matthew Digital, Security Situation in Bangladesh, (2012)
3. Mohammad Ersgadul Karim, Cyber Law in Bangladesh (2020)
4. Larisha Badeshi, ISP Liability for online defamation (2016)
5. Moore, R. (2005) "Cybercrime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.2.
6. Ahmed, Zulfiquar (2009) a Text Book on Cyber Law in Bangladesh, Dhaka: National Law Book.
7. Johannes M. Bauer, Michel J.G. van Eeten, Cyber security and Telecommunications Policy (2009) 6th Ed.

Cases:

1. United States ACLU v Reno (No 1) (1996) 929 F Supp 824ACLU v Reno (No 2) (1997) 521 US 844
2. Austin v Crystal tech Web Hosting (2005) 125 P 3d 389
3. Barrett v Rosenthal (2003) 5 Cal Rptr 3d 416
4. Barrett v Rosenthal (No 2) (2004) 9 Cal Rptr 3d 142
5. Batzel v Smith (2003) 333 F 3d 1031 (9th Cir)
6. Blumenthal v Drudge and AOL, Inc. (1998) 992 F Supp 44
7. Cubby Inc. v CompuServe Inc. (1991) 776 F Supp 135
8. Doe v GTE Corp (2003) 347 F.3d 655 (7th Cir)
9. FCC v Pacifica Foundation (1978) 438 US 726
10. Gentry v eBay, Inc. (2002) 121 Cal Rptr 2d 703
11. Grace v eBay (2004) 16 Cal Rptr 3d 192
12. Green v Am Online, Inc (2003) 318 F 3d 465 (3rd Cir)
13. Kenneth M v America Online, Inc. (No 1) (1997) 958 F Supp 1124
14. Kenneth M v America Online, Inc. (No 2) (1997) 129 F 3d 327 (4th Cir)
15. Lehman v Chuckle berry Publishing, Inc. (1981) 521 FSupp228
16. MAI systems v Peak Computer (1993) 991 F 2d 511 (9th Cir)

17. Raytheon Co v John Does 1-21 Civil Action No 99-816 (Commonwealth of Massachusetts Superior Court, Middlesex County, Filed Feb 1, 1999)
18. Red Lion Broadcasting Co v FCC (1969) 395 US 367
19. Religious Technology Centre v Netcom, Inc. (1995) 907 F Supp 1361
20. RIAA v Verizon (No 2) (2003) 351 F 3d 1229 (DC Cir)
21. RIAA v Verizon (No1) (2003) 240 F Supp2d 24
22. Schneider v Amazon.com (2001) 31 P 3d 37
23. Stratton Oakmont Inc. v Prodigy Services Co (1995) 23 Media L Rep 1794
24. Civil Aviation Dept. v Mackenzie [1983] NZLR 78 (CA)
25. Department of Internal Affairs v Young [2004] DCR 231
26. Godfrey v Telecom New Zealand 1997-G-No 107182

Statutes:

1. Digital Security Act, 2018.
2. ICT Act, 2006.

Other sources:

1. Prothome Alo, HC orders removal of fake news from Facebook, YouTube (31 Aug,2022)
2. The daily Star, Digital Security Act: Misused to muzzle dissent, (Feb 2021).