International Journal of Law
ISSN: 2455-2194; Impact Factor: RJIF 5.12
Received: 20-01-2020; Accepted: 21-02-2020; Published: 22-03-2020
www.lawjournals.org
Volume 6; Issue 2; 2020; Page No. 128-134

Changing dynamics of the liabilities of intermediaries in cyber space

Aishwarya
Assistant Professor, Indian Instituite of legal studies, Afiiliated from Uviversity of north Bengal, Silliguri, West Bengal, India

Abstract
The present research work on the topic of "Liabilities of intermediaries in cyberspace" is both explorative and analytical. It sought to construct, throughout the analysis of secondary data. The documents of government policy, financial data, and financial static provided by international authorities are analyzed and try to find out the changes and loopholes in it. Online intermediaries are entities that facilitate all of the transactions that take place on the internet. The extent of the data that flows through such intermediaries on a daily basis presents several privacy concerns, which are the subject of this Report. In my research work I am going to discuss about the data privacy laws. Obligation imposed on intermediaries while handling the data, as India has adopted the conditional "safe harbor" approach in 2008 by amending the Information Technology Act 2000 to modify the safe harbor provision contained in Section 79. I will be highlighting some leading case laws relating to data protection laws in India and also how the legislature must specify the extent to which the privacy principles will apply to data held by the Government, as well as put in place adequate checks and balances to reign in the Government's ability to intercept or modulate content hosted by intermediaries.

Keywords: intermediaries, liability, information technology, cyberspace

Introduction
The world today is a connected world. Not only large numbers of legal entities connected to the Internet, but they also offer various kinds of services on computer networks and the Web. Such service providers typically handle third-party data as well as providing platforms where such third-party data are generated, published, stored, transmitted or hosted in any network. Online intermediaries are entities that facilitate all of the transactions that take place on the internet. The extent of the data that flows through such intermediaries on a daily basis presents several privacy concerns, which are the subject of this article. This article seeks to achieve this purpose. First, it will trace the evolution of the right to privacy, and apply it to the context of an individual's transactions on the internet. Next, the Report will comprehensively document the extent to which the right to privacy is recognized in India, based primarily on the Supreme Court's jurisprudence. Thereafter, it will analyze the obligations imposed on intermediaries in India in order to safeguard the right to privacy.

Meaning of Cyberspace
The computer's ability to share data with other computers over a network linked through telephone has led to a major telecommunication revolution. A computer network is a network consisting of a central computer usually known as server and a number of mote stations say 20-30 reporting to it. Networking has led to the concept of cyberspace. It is a term used to describe a 'computer world' created by the connection of computers and the computer networks. The resulting whole is a decentralized, global medium of communication that links people, institutions, corporations and governments.

1.1 The Concept of Privacy in different aspect
Developing privacy safeguards has never been the subject of a real global coordination initia eveloping privacy safeguards has never been the subject of a real global coordination initia Developing privacy safeguards has never been the subject of a real global coordination initia cDeveloping privacy safeguards has never been the subject of a real global coordination initia.

Developing privacy safeguards has never been the subject of a real global coordination initiative and this can be for a number of reasons. Indeed, privacy is hardly a homogeneous concept. Its subjective character makes it rather difficult to establish a concept of privacy that's both broad enough to encompass its several manifestations and specific enough to be really useful which is, in fact, the only reason to bring a concept into life. Even some of the most widespread concepts of privacy for instance, that of the "right to be let alone," although being a milestone, only catches part of its actual significance. Thus, privacy ended up being conceived and enforced by Law in a variety of ways, relying on legal frameworks and tools that are particular to each country's legal system and with no real urge for global coordination [1].

The roots of the concept of privacy may be traced as far back as the teachings of Aristotle in ancient Greece, in the distinction he drew between politics (polis) and the domestic space. Over time, this concept has evolved into two distinct legal forms: (i) as an action for damages under tort law, as in cases where one's privacy has been unlawfully invaded; and (ii) constitutional recognition of individuals' right to privacy against unlawful Government intrusion. Under tort law, William Prosser's pioneering definition of privacy was based on the nature of the conduct and injury caused in each case (e.g., unfair intrusion into the seclusion of the individual, theft of name or similarity,

[1] J.Q. Whitman, "The Two Western Cultures of Privacy: Dignity Versus Liberty," Yale Law J., vol. 113, no. 6, 2004, pp. 1151–1221.

bringing undue attention to the personal life of the individual, and advertising in the false light) [2].

By and large, the concept of privacy is specific to a country, to a culture, and to an historical period, and privacy rights generally encompass the set of these cultural and historic aspects tied to this concept. As for data protection, it's a more pragmatic approach, under the rationale that it aims to safeguard individuals by protecting something that's exterior to them, their personal data. Furthermore, rules to govern data can be much more concrete and bound for global harmonization than privacy rights.

If we add to legislation the set of other elements to be taken into account, such as the implementation of technologies, industry's best practices, and even the different degrees of enforcement of data protection laws provided by Data Protection Authorities (DPAs), we can conclude that it is, indeed, possible to have completely different outcomes in enforcement even with similar legislation in place [3].

The right to privacy is now recognized internationally as a basic human right, and several international treaties and agreements create an obligation to protect the privacy of individuals. One such instrument, the Universal Declaration of Human Rights (UDHR) [4] was adopted by the United Nations (UN) in 1948, and represents the first comprehensive agreement between nations on the specific rights and freedoms of all human beings. India voted in favor of Article 12 of the UDHR, which lays down the right to privacy by specifying that a person would have the right to protect the law from arbitrary interference. In 1979, India ratified the International Covenant on Civil and Political Rights (ICCPR). 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 honor and reputation," and that everyone has the right to protection of the law against such interference or attacks. [5]

Nonetheless, India has not signed the First Optional Protocol to the ICCPR, and thus it is not necessary for Indian citizens to make a complaint or "contact" to the UN based on India's failure to fully implement Article 17 of the ICCPR. [6]

As per Section 66E of the Information Technology Act, 2000. The term privacy has been restricted to the images of private areas of a person.

Section: 66(E)-Punishment for violation of privacy Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both Explanation.- For the purposes of this section– (a) "transmit" means to electronically send a visual image with the intent that it be viewed by a person or persons; (b) "capture", with respect to an image, means to videotape, photograph, film or record by any means; (c) "private area" means the naked or undergarment clad genitals, pubic area, buttocks or female breast; (d) "publishes" means reproduction in the printed or electronic form and making it available for public; (e) "under circumstances violating privacy" means circumstances in which a person can have a reasonable expectation that–

(i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or

(ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place [7]. But,if we look at Article 21 of the Constitution of India as interpreted in R. Rajagopal v. State of T.N [8] popularly known as "Auto Shanker case", the Supreme Court has expressly held " the "right to privacy", or the right to be let alone is guaranteed by Article 21 of the Constitution. A citizen has a right to safeguard that privacy of his own, his family, marriage, procreation, motherhood, child-bearing and education among other matters. None can publish anything concerning the above matters without his consent whether truthful or otherwise and whether laudatory or critical. If he does so, he would be violating the right of the person concerned and would be liable in action for damages. However, position might differ if he voluntarily puts into controversy or voluntarily invites or raises a controversy." Thus, the Information Technology (Intermediaries guidelines) Rules, 2011 has given a broad list of content considered to be unlawful, that are replete with ambiguous terms.

Review of the Law on Privacy

The IT Act 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 put into place fairly detailed guidelines that dictate the operations of an intermediary while collecting and handling data. The introduction of these Rules in 2011 was primarily the result of privacy concerns raised when the telephonic conversations with various industrialists and politicians were leaked to the press. [9] Nevertheless, driven by concerns that the these provisions were insufficient to deal with broad privacy concerns in the context of the modern internet, a Group of Experts on Privacy [10] was constituted by the Planning Commission of the Government of India to identify key privacy issues and prepare a foundation for a new Privacy Bill aligned with the international landscape of privacy laws, global data flows, and privacy concerns that have arisen with rapid technological advancements. After analysing the international law pertaining to privacy [11] and

[2] William L. Prosser, Privacy, 48 CAL. L. REV.383 (1960).

[3] K.A. Bamberger and D.K. Mulligan, "Privacy in Europe: Initial Data on Governance Choices and Corporate Practices," The George Washington Law Rev., vol. 81, no. 5, 2013, pp. 1529–1664.

[4] G.A. Res. 217 (III) A, Universal Declaration of Human Rights (Dec. 10, 1948).

[5] This language is similar to Article 8(1) of the European Convention on Human Rights 1950, which provides that "everyone has the right to respect for his private and family life, his home, and his correspondence."

[6] Graham Greenleaf, Promises and Illusions of Data Protection in Indian Law, 1.1 INTERNATIONAL DATA PRIVACY LAW 47.

[7] The Information Technology Act, 2000.

[8] R. Rajagopal v. State of T.N 1995 AIR 264, 1994 SCC (6) 632.

[9] ITDG Bureau, India needs law against invasion of privacy: Ratan Tata, INDIA TODAY (Feb. 16, 2011), http://indiatoday.intoday.in/story/india-needs-law-against-invasion-of-privacy-ratantata/1/130050.html.

[10] The Group of Experts on Privacy was chaired by Justice AP Shah, former Chief Justice of the Delhi High Court, and its members included representatives from the Planning Commission and the Department of Personnel & Training under the Government of India, industry bodies such as NASSCOM and DSCI, academia and research centres such as Centre for Internet and Socimety, and media outlets such as NDTV.

[11] Including the OECD Privacy Guidelines, EU Data Protection Directives, APEC Privacy Framework, Canada Personal Information Protection and Electronic Documents Act (PIPEDA), and Australia National Privacy Principles (ANPP).

comparing it with the existing privacy jurisprudence in India, the Expert Group published a 92–page report making recommendations to streamline the law pertaining to data protection and privacy in India [12]. At the outset, the Group of Experts recognized that the need for regulation stems from the economic value of data, and that global data flow generates value for the individual as a data creator and for businesses that collect and process such data. Therefore, the Expert Group stated that the objective "should be to put into place a regulatory framework for both public and private sector organizations. The ambit of the privacy legislation will extend to data being processed within India, and data that originated in India, even when it is transferred internationally. [13]

It was recognized that the fundamental philosophy underlying these principles is the need to ensure transparency, enforceability, and accountability for the collection, processing, and use of data, thereby ensuring that the privacy of the concerned individual is guaranteed. The conception of the Privacy Principles by the Group of Experts appears to be a departure from the "third party doctrine" in the U.S., and is based on the idea that the information forms a part of the individual and his dignity, and therefore ought to be protected. While the existing provisions contained in the IT Act and Rules do serve to achieve the ends of the nine Privacy Principles to some extent, the Group of Experts identified and recommended a number of ways in which the Privacy Bill could improve upon the laws relating to data protection. Among other measures, the Group recommended that the proposed privacy legislation should apply to both the private and public sectors, and to all data processed in India even if it is subsequently transferred to another jurisdiction [14],

Privacy Bill 2014

Based on the recommendations of the Group of Experts, the Government has attempted to rework the privacy and data protection laws in India by preparing a draft Right to Privacy Bill 2014. [15] Heeding the recommendation of the Group of Experts, the Bill explicitly recognizes that the right to privacy is a part of the right to life under Article 21 of the Constitution. The nine Privacy Principles are enumerated in the Schedule to the Bill, and its provisions give effect to the Principles in such a way that elevates the data protection law in India to be virtually on par with the regime in Europe, and requires that all personal data mandatorily disclosed to intermediaries be processed according to the Bill. [16] The Privacy Bill will apply to any person who "shall collect, process, or otherwise deal with personal data of any individual" (all residents of India, and not merely citizens of India). A data controller who does not maintain a place of business in India but who collects and handles the personal data of any Indian resident must nominate a representative resident in India who will be responsible for compliance. It is unclear whether all overseas data controllers who collect data from residents in India may be compelled to nominate a representative resident in India or the consequences if a data controller fails to appoint such a representative.

1.2 What are the intermediary liabilities?

Definition of Intermediary

An intermediary in the context of the Internet can be understood as an entity that acts as a facilitator of the flow of data across the vast and complex synapses of the Internet. While the actual functions of intermediaries are dynamic and often not clear-cut, they can broadly be seen as falling into one of two categories i.e. conduits for data traveling between nodes of the Internet, hosts for such data [17].

The Organization for Economic Co-operation and Development (OECD) in April 2010 proposed that "Internet intermediaries" be defined as follows:

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 [18].

Some national jurisdictions on the other hand, have chosen to not attempt defining the term "intermediary" as such in relevant laws. Instead, broader alternate terms like "information society service [19] and "interactive computer services" are employed, and intermediary regulations are incorporated into law without referencing the term "intermediary".

According to Section 2(1)(w) of the IT Act therefore, an intermediary is any person who receives, stores or transmits an electronic record on behalf of another person or provides any service with respect to that record [20]. The Section then clarifies that the term includes telecom service providers, network service providers, Internet service providers, web hosting service providers, search engines, online payment sites, online auction sites, online marketplaces and cyber cafes.

1.3 Enlargement of the safe Harbour coverage range

The Indian Government enacted the IT Act to provide legal recognition to e-commerce, to facilitate electronic filing of documents with government agencies and amend other existing laws like the Indian Penal Code, 1860 and the Indian Evidence Act, 1872. This was based on the UN General Assembly adopting the Model Law on Electronic Commerce issued by the United Nations Commission on International Trade Law, [21] to which India was a signatory. According to the Statement of Objects and Reasons of the

[12] Justice Ajit Prakash Shah, Report of the Group of Experts on Privacy, PLANNING COMMISSION OF INDIA (2012), http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf.
[13] Id.
[14] *Id*.
[15] The draft Privacy Bill 2014 has not yet been made public. For analytical purposes, this Report has relied on articles written by CIS discussing the provisions of the Privacy Bill. See, e.g., Elonnai Hickok, Leaked Privacy Bill: 2014 vs. 2011. The centre for internet and society (Mar. 31, 2014), http://cis-india.org/internet-governance/blog/leaked-privacy-bill-2014-v-2011.
[16] Graham Greenleaf, India's draft The Right to Privacy Bill – Will Modi's BJP Enact It?, 129 PRIVACY LAWS & BUSINESS INTERNATIONAL REPORT 21 (2014), http://ssrn.com/abstract=2481796.
[17] APC, Frequently asked questions on Internet Intermediary Liability, ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS, https://www.apc.org/en/pubs/apc%E2%80%99s-frequently-asked-questions-Internet-intermediary.
[18] OECD, Definitions, 9, THE ECONOMIC AND SOCIAL ROLE OF INTERMEDIARIES 2010.
[19] Directive (EU) 2015/1535 of the European Parliament and of the Council, laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, Available at: https://eurlex.europa.eu/legal-content/EN/TXT/?qid=1551937833098&uri=CELEX:32015L1535.
[20] Information Technology Act 2000 Section 2(w).
[21] General Assembly of the UN, resolution A/RES/51/162 dated January 30, 1997

IT Act, "There is a need for bringing in suitable amendments in the existing laws in our country to facilitate e-commerce. It is, therefore, proposed to provide for legal recognition of electronic records and digital signatures.

Section 79 is currently the provision that guarantees safe-harbour protection to intermediaries for third party content. Section 79 of the original Act only protected network service providers [22] from liability arising from third party content, if they proved absence of knowledge; or application of positive application of due diligence on their part to prevent commission of an offence/ contravention.

Subsequently, an amendment to the IT Act in 2008 [23] ("the IT Amendment Act") made substantial changes to Section 79 (the safe-harbour provision) and the definition of intermediaries. One of the triggers for amending the IT Act in 2008, specifically for widening the protection given to intermediaries, was the MMS scandal affecting Baazee.com (at that time, a wholly owned subsidiary of Ebay Inc. USA). In this case, an MMS clip was listed on Baazee.com (an e-commerce website) which contained sexually explicit content which was being offered for sale on the website.

The IT Amendment Act enlarged the definition of the word 'intermediary' to service providers like telecom service providers, Internet service providers, search engines, online marketplaces and even cyber cafes. It also widened the safe-harbour protection given to these intermediaries under Section 79 [24] from only network service providers to all intermediaries and protected intermediaries from all unlawful acts rather than offences and contraventions covered under the IT Act itself.

How do the intermediary rules operate?

The new intermediary rules mandate the intermediaries to impose a set of rules and regulations on users. The rules further specify the terms of such regulations and this includes a broad list of categories of content which should not be posted by users. The broad list of unlawful content includes information that is grossly harmful, harassing, blasphemous, defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever. These words are too ambiguous and result in broad interpretation. Now, any person aggrieved by any content on the internet can ask the intermediaries to take down such content. Intermediaries are obliged to remove access to such content within a period of 36 hours from the time of receipt of the complaint. The rules do not provide for the creator of the content to respond to this complaint. In fact, the rules do not even provide for the intermediaries to inform the user who posted the content regarding the complaint. The intermediaries that do not comply with take-down notice loses the protection from any legal liability that could arise over user content.

A legal analysis of the Information Technology (Intermediaries guidelines) Rules, 2011

The Government has notified on April 13, 2011 the Information Technology (Intermediaries guidelines) Rules, 2011 prescribing guidelines to be observed by the intermediaries. The rules were issued in exercise of the powers conferred by clause (zg) of subsection (2) of section 87 read with sub-section (2) of section 79 of the Information Technology Act, 2000 (Act 21 of 2000). The provisions of the new rules are unconstitutional as they affect the right to freedom of speech and expression as well as right to privacy of citizens, are arbitrary being violative of Art. 14 of the Constitution of India and are ultra vires of the parent act. Section 79 of the Act provides the intermediaries protection from liability arising out of user generated content. This is in line with the position followed in countries like the US and members of the European Union. The Digital Millennium Copyright Act and the Communications Decency Act in the US and the Directive on Electronic Commerce in the EU provides protection to intermediaries from liability arising out of content posted by users of services provided by intermediaries. S. 79 of the Act mandates the intermediary to observe due diligence while discharging its duties under the Act and to observe such other guidelines as prescribed by the Central government in this behalf. The Central Government is thus conferred with powers to prescribe guidelines relating to duties to be discharged by the intermediaries. However while issuing this sub-ordinate legislation, the central government has acted beyond its powers provided under the Act and expanded and amended the provisions of the Act.

Guidelines for Attaining Safe-Harbour

Following the 2008 amendment to the IT Act introducing the ' due-diligence ' clause for intermediaries to demand safe harbour, on 11 April 2011 the Government of India released the 2011 Rules on Information Technology (Intermediaries Guidelines). The Intermediaries Guidelines, inter alia, brought in the following conditions, which all intermediaries had to adhere to for their safe-harbour protection [25].

a. Publishing rules/regulations; privacy policies; user agreements;
b. Terms and conditions to specify prohibited content-grossly harmful, harms minors, infringes intellectual property rights, contains virus (among other things).
c. A strict notice and takedown process;
d. Assistance to government agencies for law enforcement;
e. A duty to report cyber security incidents to the government; and
f. Appointment and notification of a grievance officer.

Weathering state intervention

Besides issues arising from the processing and use of data b y private entities, the use of data by the government often ne eds oversight, including when the government collects and r etains data for electoral databases and universal identity car ds, as well as situations where the government intercepts dat a from private entities. This dynamic exists because in India, the constitutional jurisprudence on the right to privacy suggests that it is subject to reasonable restrictions, if such restrictions are in furtherance of the interest of the security of the State. Any such action is bound to conflict with internet users' right of privacy; although such situations are not yet frequent occurrences in India, the possibility of State

[22] According to the previous Section 79 of the IT Act, network service providers meant - 'intermediaries' as defined under the Act.
[23] The Information Technology (Amendment) Act, 2008.
[24] Section 79 of the IT Act.
[25] To refer to the entire text of the Intermediaries Guidelines, kindly refer to https://www.wipo.int/edocs/lexdocs/ laws/en/in/in099en.pdf

intervention similar to that seen in instances across the world looms large. Intermediaries operating in India are subject to myriad laws and mechanisms which permit State oversight over the content hosted by them. In "The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights" (OHCHR), emphasis has been placed on the role played by private intermediaries in facilitating surveillance. [26]

The IT Act 2000 contains provisions which vest in the Government the power to issue directions to intercept, monitor, and collect information that flows through "computer resources." Section 69 empowers the Government to "direct any agency of the appropriate Government to intercept, monitor, or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource," if it finds that it is necessary or expedient to do so in the interest of "the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence." In addition, Section 69B empowers the Government to "monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource," in order to "enhance cyber security and for identification, analysis and prevention of intrusion or spread of computer contaminant in the country." "Traffic data" has been defined in Explanation (ii) to Section 69 B as "any data identifying or purporting to identify any person, computer system or computer network or any location to or from which communication is or may be transmitted."

Intermediary Liability in Reality

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

Then there is the reality that bad actors use online platforms to disseminate disinformation, terrorist content, child porno graphy, etc., forcing governments around the world to hold i ntermediaries more accountable on their platforms for third party content. Countries across the world are pressuring intermediaries to be more responsible for the content flowing through their platforms. Though intermediary liability needs to be revisited in the current global context, any changes to law and regulation must ensure that it doesn't abrogate basic human rights. Content takedown requests are sometimes also received by intermediaries in the form of orders of law enforcement agencies under Section 91 of the Code of Criminal Procedure,1973 ("CrPC") [27]. The IT Act, gives enough powers to central and state governments for intercepting, monitoring, decrypting and taking down content from their platforms. [28]

Intermediary Liability and IP Disputes in India

The intermediary liability law in India is primarily governed by Section 79 of the IT Act as discussed above. As per that provision, online intermediaries enjoy a safe-harbour for third-party content on their platforms, till they prescribe to certain due diligence rules set out under the Intermediaries Guidelines. Provisions under the Copyright Act, 1957 provide for some protection to certain intermediaries as well. [29] Section 79 of the IT Act in conjunction with the ruling of the Supreme Court of India in Shreya Singhal, which broadened the protection given to intermediaries and allowed them to takedown content only on instructions by courts or authorized government agencies, is the authoritative law of the land on intermediary liability. Though, it is important to point out that in terms of intellectual property rights ("IP rights"), courts in India have placed a higher responsibility on intermediaries to take down content content that infringes IP rights.

Intermediary liability in other jurisdictions

Different jurisdictions may establish different enactments and procedures to restrict content that is considered unlawful. Different regimes also follow different legal frameworks to grant conditional immunity or safe harbour to intermediaries. The notice and notice model obliges intermediaries to direct any complaint of alleged infringement of copyright they get from the owner of copyright to the user or subscriber in question. This procedure is followed in Canada and is enshrined in the Copyright Modernization Act, that came into effect in January, 2015. According to this model, receiving a notice does not compulsorily mean that the subscriber has infringed copyright and does not require the subscriber to contact the copyright owner or the intermediary.

Right to Be Forgotten in the EU

The GDPR came into force on May 25, 2018, repealing the 1995 Data Protection Directive. It is meant to harmonize data privacy laws across Europe, protect data privacy of EU citizens and provide a comprehensive data privacy framework for organizations that collect and process data. [30] Article 17 of the GDPR provides for the Right to Erasure or the Right to be Forgotten. This is a development from the Data Protection Directive where there was no mention of this term, although it was implicit under Articles 12 and 14. The grounds under Article 17 of the GDPR are detailed and broader than those provided in the 1995 Data Protection Directive. The data subject has the right to demand erasure of the information concerning her in the following cases:

- personal data is not required for processing;
- she withdraws consent;
- when there has been unlawful processing of data;
- objection is on grounds under Article 21(1) and Article 21(2) of GDPR; [31]

[26] U.N. High Commissioner for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37 (2014).

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

[28] Section 69 and 69A of the IT Act.

[29] Section 52(b) and (c) of the Copyright Act, 1957.

[30] The European Union General Data Protection Regulation, (9 Jan, 2020, 2:49 PM).

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

- national laws require erasure of data and; and
- when the data is provided in relation to information society services by a child under Article 8(1). [32]
- The Article also provides for situations in which the Right to be Forgotten will not be applicable.

Judiciary analysis on intermediary liability

- Having gone over the applicable laws with regard to intermediary liability in India, this section of the report will examine some of the notable cases around intermediary liability in India. Only cases from various High Courts (at the state level) and the Supreme Court of India have been considered for this section, and the list is non-exhaustive. The cases discussed herein are relevant to provide an overview of the jurisprudence which has evolved in India on issues surrounding intermediary liability. [33] Therefore, the objective of the notice-and-notice regime is to discourage online infringement on the part of Internet subscribers and to raise awareness in instances where Internet subscribers' accounts are being used for such purposes by others. [34] It enables the complainant and the content owner to resolve the dispute among themselves without the involvement of the intermediary. The second model is the notice and takedown model. It is followed by countries like South Korea [35] and the United States of America. [36] According to this system, an intermediary responds to government notifications, court orders or notices issued by private parties themselves, to take down content by promptly removing or disabling such allegedly illegal content. This self-regulatory framework, by which ISPs determine whether or not a website contains illegal or harmful content raises questions of accountability, transparency and the overall appropriateness of delegating content regulation to private actors, who have to act as judges. [37] The law relating to intermediary liability in the United States of America is mostly governed by Section 512(c) of the Digital Millennium Copyright Act ("DMCA") and Section 230 of the Communications Decency Act ("CDA"). Section 512 of the DMCA was enacted by the US Congress with a view to limit the liability of intermediaries and to check online and copyright infringement, including limitations on liability for compliant service providers to help foster the growth of Internet-based services. [38] The intermediary must comply with the notice-and-takedown procedure under Section 512 to qualify for protection.

Indian courts on intermediary liability

Having gone over the applicable laws with regard to intermediary liability in India, this section of the report will examine some of the notable cases around intermediary liability in India. The cases discussed herein are relevant to provide an overview of the jurisprudence which has evolved in India on issues surrounding intermediary liability. Shreya Singhal v. Union of India (2015)

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

Myspace Inc. vs. Super Cassettes Industries Ltd. (2017) [39]

This case is important from a copyright perspective as the division bench of the Delhi High Court in this matter reversed a single judge decision holding Myspace liable for copyright infringement. The division bench held that if intermediaries are tasked with the responsibility of identifying illegal content, it could have a chilling effect on free speech. For a detailed discussion on what the court held in Myspace, kindly refer to the section 3.1. In this matter, the court also distinguished the 'actual knowledge' requirement from Shreya Singhal to mean 'specific knowledge' in matters of copyright infringement i.e. if intermediaries are pointed to specific infringing material by rights holders then they must remove such content, without the necessity of a court order.

Conclusion

Increase in the number of users of online platforms that allow sharing of user generated content coupled with a lack of media literacy have led to an explosion of harmful content ranging from hate propaganda to disinformation to revenge porn and child pornography. he spread of disinformation is contained. The initiative of intermediaries in working together with fact checkers across the world is a positive move and will improve the trust of users in the content shared. The trust deficit of online platforms and incidents attributed to harmful content spread online have been used by Governments in various countries as excuses to justify new regulations that seek to control information on these platforms. In India, the Shreya Singhal judgment has given intermediaries the much needed certainty on the requirements for enjoying safe-harbour protection. However, the proposed amendments to the Intermediaries Guidelines Rules endangers this protection. Attempts at regulating intermediaries by weakening encryption or by mandating automated take-down on a broad range of content deemed to be harmful will be counterproductive and will affect the fundamental rights of free speech and privacy guaranteed to citizens. However, a laissez faire approach permitting intermediaries complete freedom is also not advisable as the real-world harm caused by illegal content cannot be ignored. Governments should be free to mandate intermediaries to ensure quick resolution of legitimate takedown requests and to have in place governance structures and grievance mechanisms to enable this.

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

[33] The US Copyright Modernization Act 2015.

[34] Office of Consumer Affairs (OCA), Notice and Notice Regime, Innovation Science and Economic Development Canada (Mar 9, 2019, 1:48 PM), https://ic.gc.ca/eic/site/oca-bc.nsf/eng/ca02920.html.

[35] The South Korea Copyright Act 1957 § 103.

[36] Digital Millennium Copyright Act 1998 § 512(c).

[37] Christian Ahlert, Chris Mrasden and Chester Yung, How Liberty Disappeared from Cyber space: The Mystery Shopper Tests Internet Content Self Regulation, THE PROGRAMME IN COMPARATIVE MEDIA LAW AND POLICY, UNIVERSITY OF OXFORD (9 Mar, 2019, 2:00 PM), http://pcmlp.socleg.ox.ac.uk/wp-content/uploads/2014/12/liberty.pdf

[38] The US Copyright Modernization Act 2015 U.S. Copyright Office, Section 512 Study, COPYRIGHT.GOV (9 Mar, 2019, 2:04 PM), https://www.copyright.gov/policy/ section512/

[39] Myspace Inc. vs. Super Cassettes Industries Ltd. [236 (2017) DLT 478]

References

1. The Information Technology Act, 2000.
2. Rajagopal RV. State of TN 1995 AIR 264. 1994; (6)632.
3. To refer to the entire text of the Intermediaries Guidelines, kindly refer to https://www.wipo.int/edocs /lexdocs/ laws/en/in/in099en.pdf
4. The US Copyright Modernization Act, 2015.
5. Office of Consumer Affairs (OCA), Notice and Notice Regime, Innovation Science andEconomicDevelopment Canadahttps://ic.gc.ca/eic/site/ocabc.nsf/eng/ca02920.html.
6. The South Korea Copyright Act, 1957, 103.
7. US Digital Millennium Copyright Act, 1998, 512(c).
8. Christian Ahlert, Chris Mrasden and Chester Yung, How Liberty Disappeared from Cyber space: The Mystery Shopper Tests Internet Content Self-Regulation, the programme in comparative media law and policy, university of oxford (9 Mar, 2019, 2:00 PM), http://pcmlp.socleg.ox.ac.uk/wp- content/uploads/ 2014/12/liberty.pdf.
9. Myspace Inc. vs. Super Cassettes Industries Ltd. [(2017) DLT 478].