Expression Through Socialising Media in India: Why Fixing the Existing Legal Dilemmas Is Critical?

Meera Mathew

Assistant Professor, Symbiosis Law School, Deemed University, PhD. Address: NOIDA Sec-62, Block-A, 47 & 48, NOIDA (PIN-201301), Uttar Pradesh, India. E-mail: meera@symlaw.edu.in

Abstract

The emergence of the social media and its virtual communication space has enabled people at large to interact and communicate from the conventional mode of one-to-one to many-to-many. It exploded onto the technology in the last decades for commercial and entertainment purpose and rapidly it had become very much prevalent globally. Initiated as a friend-finder it went on to the extend encompassing every features of media where the users had a dominant role. When mass media and digital media was through certain modes, social media not only changed the mode but the creators and audience. From passive news listeners, it became active creators and sharers of contents in the form of information. With the enablement of technology, anybody with an internet access and own opinion can be part of social media. Under the guise of user-generated content, be it in sharing of news or opinion or images or videos and now even the live video promoting political, social, cultural aspects, social media do not hold any accountability because only users are producing contents. Also, being an intermediary, it is free from any liability for the user generated data under Indian Information Technology Act, 2008 and the existing global consensus under safe harbour doctrine. The law in this area is still relatively unsettled. The misuse of social media got reported with various incidents of such as impersonation, anonymity, profile account hacking, privacy threats, sexual or aggressive solicitation, cyber-bullying, and many such related serious issues. However, in all these matters, social media was provided with a benefit for its passive involvement of choosing the users or the contents posted. The liability was always on the content producers. It is certain degree of due diligence social media platform needs to observe that too very minimal! This paper endeavours to question the existing privilege available to social media at par with conventional media and also highlights the social-legal dilemma it put forth with unprecedented use of data. It further dwells upon the legal impediments in challenges that social media pose for the lack of legislation- especially for data protection and user profile anonymity detection. It thus attempts to find out whether social media is to be equated like media or should it be viewed as mere platform for people to express. If it is just a platform to express, whether the current Indian legal framework is sufficient enough, to deal with the ramifications arising out of social media especially when most of them are social media companies incorporated and registered under foreign jurisdictions.

Keywords
expression, social media, legal issues, Indian legal system, Information technology.

For citation: Meera M. (2020) Expression through "Socialising" Media in India: Why Fixing the Existing Legal Dilemmas is Critical? // Legal Issues in the Digital Age, no 3, pp. 97–124.

DOI: 10.17323/2713-2749.2020.3.97.124

Introduction

The internet service websites, blog pages, mobile technologies, social media and networking sites web have entirely altered previously prevailed communication model. The internet, digitalization and social media are transforming news from its traditional practice from its original notions of press and media. The degree at which exchange of communication existed had been multi-folded with sudden increase in information collected and circulated. Today every news-media has its social media webpage including *Twitter* handles or *Facebook* pages thus stories are searched on internet service providers to know if any user has uploaded anything that became 'viral'. Moreover, it has become a necessity for mainstream print media to have their websites, live videos, journalists' blogs, invited newsrooms debates where invitation is extended to community participation [Knutson A., 2009: 437–474].

The bloggers consider themselves as journalists and break *scoops* and stories. With notable shift to mobile news access news has now become omnipresent-available on every platform at any time. Regardless of their professions, resources or training today, *netizens* are disseminating news to the public themselves. Personalized and participatory stories having maximum views or shares are now converted as news.

Further the technological changes and ongoing perception of news", its practices of reporting are greatly influencing at its quantity, quality and nature of reporting, whether online or in print. While print media still have a noteworthy readership, the digital media and new media sites have clearly had a fading impact on the print medium. Social media has divulged in innovative ways to interconnect and collaborate the population through technology. Smart-phones and tablets have redefined customer computing and provide instantaneous access to information from any locality. For instance, observe the development and muti-fold uses of a smart phone [McPeak A., 2015: 235–292]. On it, one can listen to music, phone people, text, watch videos, send and receive emails, surf the internet, play games, watch videos, store pictures and plan the travel with calendar and many other things. Instead of carrying disc-man, walk-man, laptop, diary, camera, telephone today all in one is possible. This is the convergence where all contents and in-

formation is carried by one tool [De Sola P., 1983: 76]. The much notable characteristic of social media is the upsurge in 'citizen journalism', under which individuals determine what could be the news and accordingly publish it via blog or platforms and disseminate the same unlike the earlier prevalent mainstream journalism. This has created a discrepancy in the online communication (often equated to 'chatting' from one to one) the social communication where (any tweet or Facebook post is as much a publication as a newspaper article from one to many or many to many). The commencement of an online-based 'activism' accompanied by the Web 2.0 technology conveys an occasion for its collaborating platform, includes blogs and social network sites an online skill for users to stimulate a profile — public or semi-public, with a view to network with other whom they share a conjoint relationship, and traverse others' profiles and networks. This content creation can turn out to be adverse, menacing or can have a prospective to stir up a rebellion.

The internet as a whole and social media in particular exaggerate the possibility for contents to initiate riot just by taking the circumstances out of the background and using it or even manipulatively generating it. Similarly, it is to be seen how far the privacy constraints are trespassed. Unlike the normal media, it is perplexing for the mass dynamics to enforce a similar controlling impact on social media, which goes on to another argument for why social media need to be regulated like traditional mass media. Apart from that, safe-harbor provisions where limited liability prevails for Internet intermediaries exists to be eroding the notion of traditional news media. Debates on this limited liability though raise confusion, intermediaries moot that they cannot control or regulate content online and therefore should only have restricted accountability. Given the mass quantity of data they handle, social media platforms mainly rely on report notifications from users who raise about the content if it deems misleading or unbefitting. There exists diverse global regime worldwide to determine the liability, with various impact [Stacy A., 2017: 1375]. This lack of unanimity in determining Intermediary liability is again an issue when it is a foreign company functioning in various jurisdictions having different legal scenario. Hence this necessitates to discover the issues and challenges involved in social media and examine how far Indian legal framework tried to fill the gap created by these issues. Also the case studies are done so as to analyze how other countries have done their best to resolve the same.

1. Legal Issues

1.1. Hate Speech or Inciting Posts/ Mob lynching

Speech that provokes or generates animosity adds to target, downgrade and dehumanize specific groups, resulting them to be in sidelined whereby society gets

stratified and divided. The risk of inciting speech is linked to that posed by the very crime in promoting speech. While hateful-speech cases happens in all categories of media, and should be preserved the same irrespective of the medium, the existence of the Internet, especially social media makes a difference here. There is no unanimously recognized account on hate speech. Besides, a direct association — ethical and legal consequences — cannot be recognized between the dissemination of hate speech and violence. For the very term hate makes it a subtle notion and exposed to precise exposition. It is a concept that creates misunderstanding and, given its actual nature, is temperately easy to control[1]. This makes new media to control all the writings based on hate speech.

In India the provisions to curb hate speech are laid down in different way. Under Indian Constitution, interests of the sovereignty and integrity of India", the security of the State", friendly relations with foreign states", public order", decency or morality or in relation to contempt of court", defamation or incitement to an offence are the aspects under which Art. 19(2) are applied where freedom of speech can be restricted. Apart from this, Indian Penal Code has specific sections along with specific provisions under the"Scheduled Castes and Scheduled Tribes (Prevention of Atrocities) Act, 1989; Protection of Civil Rights Act, 1955;"Indecent Representation of Women (Prohibition) Act, 1986; The Religious Institutions (Prevention of Misuse) Act, 1988; The National Security Act, 1980 etc Further there are certain specific media laws that govern hate speech that are even applicable to digital media. Despite blocking access to content under Section 69A[2], takedown of content under Section 79 of IT Act[3], 2008 and other modes of self-regulation policies are prevailing.

The question is whether the principles as adopted in offline media is to be the same for online media? The content flowing through internet-facilitated mobile phones and on social media, has reconfigured the technique in which the law, police, and civil society have coped with this issue[4]. The multinational flow of in-

[1] Law Commission of India."267th Report of Hate Speech. Delhi, 2017."

[2] S. 69 A, IT Act, 2000 states: Intermediaries failing to comply with the direction issued could be punished with imprisonment for a term which may extend to seven years and shall also be liable to fine."

[3] S. 79, IT Act, 2000 exempts intermediaries from liability in certain instances. It states that intermediaries will not be liable for any third party information, data or communication link made available by them.

[4] See S. Narain. Social media, violence and the law: Objectionable material and the Changing Contours of Hate Speech Regulation in India. *Culture Unbound*, 2018, no 3, p. 388–404. The cases of communal violence reported in India such as in Pune in 2014, in *Muzaffarnagar* in 2013, the issues cropped up at *Azad Maidan*, Mumbai in 2012, and the emigration of persons from the North-East states from cities such as Bangalore and Pune in 2012, show that the police have charged, arrested or even acknowledged those liable for acts of vehemence or making confrontational dialogues, but

formation, the effortlessness of inter-platform interchange, and the pace and scale with which information move, has challenged the conventional fact-finding and investigation procedure for police force.

The hate speech and its repercussions were first discussed exhaustively in 1919 *Schenck case*[5], where Judge J. Holmes made a difference between speech having malicious formation and speech with unintended result. By interpreting constitutional protections and dealing with the extend of harm speech can cause by elucidating proximity and degree, the"doctrine of clear and present danger test was formulated. This test though used in cases later reformulated in *Brandenburg* case, which focuses on imminent lawless action test[6]. The protections of this test, when applicable, have proven very difficult to overcome. Recently, this provision was interpreted by the US Supreme Court ruled in the case of *Anthony Elonis*[7]. With United States having a history of liberal speech with no apparent Constitutional restrictions, the judgment was merely a proposal to draw a distinction between regulating the manner of speech, as distinct from its matter!

When the offline media has been switched over to offline media, whether the same theories and principles exist is a matter of concern. Social media having the capacity to instantaneously spread messages to the crowds, unhindered by time or space, it is to be viewed seriously by law makers. Online activism can be in the method of advocacy or mobilization but there exists a thin line from advocacy to incitement. These multi-ford issues that hate speech inflicts on its targets and ap-

---

have not been competent to track dangerous speech disseminating as videos, images or text to a certain source.

[5] *Schenck* v. *United States*, 249 U.S. 47 (1919)

[6] In this, the Court held: Freedoms of speech and press do not permit a State to forbid advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action. Thus, governmental restriction on Brandenburg's speech was held unconstitutional.

[7] For more read: the case *A. Elonis* v. *United States* 135 S. Ct. 2001 (2015)". In this case, after his wife and children moved out of their home, Anthony Elonis made various postings on the internet that caused others to fear for their physical safety."Under this, the Pennsylvania amusement-park worker who took to Facebook to post violent rap lyrics aimed at his estranged wife, co-workers and the FBI agents who came to investigate him. Under the pseudonym 'Tone Dougie', Elonis went online to vent, penning lyrics such as: 'There's one way to love you but a thousand ways to kill you… Hurry up and die, bitch, so I can bust this nut all over your corpse.' The Supreme Court ruled that the original court case, which saw Elonis convicted for making online 'interstate threats', did not sufficiently prove that he intended for the posts to be threatening — an important requirement for him to be found guilty. Though circuit court found him guilty under under 18 U.S.C. § 875(c), Supreme Court did not. The Supreme Court failed to deal with the issue whether incitement and threats are subject to the same constitutional protections and, if not, why not. Further, the Court might have described the kind of subjective intent required before one could be prosecuted for either incitement or threats. Regrettably, the Court shed very little light on these constitutional questions, and its statutory analysis offered too little direction to be helpful for lower court.

propriately explains that the menace of hate speech should be weighed against the prevalent societal, cultural and the historical environment. In *Pravasi Bhalai Sangathan* case[8], the Supreme Court had examined the 'tendency' and the 'proximity' tests involved in speech and expression but left it without describing or defining the hate speech considering it as judicial overreach. Contrary to the protected and responsible speech as reflected under Freedom of speech and Right to life[9], some expressions and speech are intended to demean, overawe, or inflame violence or prejudicial action against a group of people. Finally with the Law Commission in its Report-267 stated that, certain parameters on identifying hate speech are extremity of the speech, status of the author, contents delivered, status of the victims, potentiality and context in which the speech was delieverd[10].

Coming to Mob Lynching, the statistics imply that, many are reported to have been killed in in the past few months in barbarousness fueled by *WhatsApp* messages[11]. Lynchings can be defined as extra-legal murders executed by a bunch of vigilantes who act like observants taking law in hand and with no justification kill individuals often accused of outrageous crimes. The objective behind lynching is to punish particular criminals and crimes but indirectly it also passes an unrighteous message to public to have social conformity with moral norms be it on social hierarchy, status, and gender behaviours[12]. The recent judgment of *Tehseen Poonawalla* v *Union of India and Ors*[13] where the three-Judge Bench of the Supreme Court headed by C.J. Dipak Misra had recognized the act of lynching as unlawful and in the light of growing instances of mob lynchings increased by misinformation arising out of social media messages.

This leads to the conclusion that Information being a vital element to society its distortion will have violent implications. Right to participate and right to disseminate are different. When right to participate is an affirmative right that is vested with citizens under the realm of right to know through access to certain governmental information, right to disseminate comes with inherent responsibil-

[8] *Pravasi Bhalai Sangathan v. Union of India* 2014 SCC OnLine SC 22. Available at https://main.sci.gov.in/jonew/judis/41312.pdf (accessed 03.10.2020)

[9] To be read with Article 19(2) on the grounds of public order, incitement to offence and security of the State."

[10] Law Commission of India, 267th report on Hate Speech (March, 2017)."LCI suggested for an Amendment in IPC to insert new section 153C (Prohibiting incitement to hatred) and section 505A (Causing fear, alarm, or provocation of violence in certain cases)."

[11] "Since 2017 *WhatsApp* misinformation has contributed to more than 80 different lynching incidents across India See BBC news report 12 November 2018. Available at: bbc.co.uk/mediacentre/duty-identity-credibility.pdf (accessed: 10.12.2019)

[12] Salam Z. *Lynch Files: The Forgotten Saga of Victims of Hate Crime.* SAGE, 2019, p. 120–130.

[13] Writ Petition (Civil) No. 754 of 2016.

ity. With social media, those barriers are falling and suddenly platforms generousness is helping ordinary citizens create new enterprises of all kinds. Many a times, public association in such lynchings happen due to random, silly and trivial reasons. However when the substantial law when interpreted in procedural aspects, it usually gets watered down for its strict interpretations. Ideally, for a speaker to be prosecuted for incitement, therefore, the State must show:"(i) The perpetrator/s having intention to incite another; (ii) The perpetrator/s have done something actively to cause imminent violence; and (iii) The perpetrators' overt acts were in a context that makes possible that such violence will occur.

With the criminal law interpretation of proving beyond reasonable doubt and *mensrea* to be specifically proved, it has lot of shortcomings. Secondly blocking of content online is used often to prevent the circulation of online hate speech. The process of issuing blocking orders is ambiguous, and the reasoning offered in orders is not subject to public scrutiny. This lack of transparency means there are few avenues available for the public to hold the executive accountable for misuse of its power to block online content. With the online media working under the self-regulation principle[14], what it can be done to improve the scenario to have a uniform policy for all the social media. For instance, in *WhatsApp*, the terms of use do provide that a user account, or access to the account may be modified, suspended or terminated for any reasons, including violation of the 'letter or spirit' of the terms. It also states that 'creation of harm, risk, or possible legal exposure' for *WhatsApp* can lead to the modification, suspension or termination. However, there is no reporting or other enforcement mechanism specific to 'hate speech'[15].

1.2. Jurisdiction

In the common law method, the application of jurisdiction had been founded on where the dispute is governed. With the digital media and social media the main concern was on how to govern the matters when affected parties are from different jurisdiction. The transnational nature of cyberspace, globalization of the Internet and the inapplicability of territorial jurisdiction has been challenging for nations vexing to implement at their laws in cyberspace. The past principles of *forum conveniens* or *forum non conveniens,* traditional state sovereignty, the juris-

[14] For instance, many social media in its policy advertisements prohibits 'hate speech' on race, ethnicity, national origin, colour, religion, disability, age, sex, sexual orientation, gender identity, veteran status or other protected status, inflammatory content which is likely to evoke a strong negative reaction or cause harm. See T Gelashvili, *Hate Speech on Social Media: Implications of Private Regulation And Governance Gaps* Lund, 2018, p. 27.

[15] WhatsApp Legal Info — Key Updates. Available at: https://www.whatsapp.com/legal/# key-updates (accessed: 30.09.2018)

diction concerning content hosted and passed on the internet, regulation of free flowing content on borders were the concerns. When the foreign registered company, provides Internet users with access to various services beyond geographic boundaries the applicability of laws and regulations was a challenge

Jurisdiction denotes the dominion of a court to listen to a matter and determine the case. Deprived of jurisdiction, a court's finding becomes futile and powerless. The Internet generates uncertainty for sovereign territory since system restrictions traverse and surpass state boundaries. Under international law 'jurisdiction' is sometimes referred to as the law of 'extraterritorial' jurisdiction. The extraterritoriality also poses a challenge for judicial cooperation, in as much as legislative differences also affect very important questions relating to cyber-crime, such as data protection and communications secrecy. Additionally, it poses difficulties that arise from the technical conformation and functionality of the Internet (such as on server setting, IP validation, various encrypting dealings for concealing identity from spam outbreaks, etc.) that causes a number of indecisions and complications in procuring evidence or outlining accountability.

Even trans-boundary defamation upsurges a range of concerns, especially the private international law demands about which courts should adjudge matters and what would be the applicable law. A defamatory statement if appears online it can be published wherever internet is accessible. The decision of a French trial Court to *Yahoo Inc*. to install filtering system to avoid people from offering to sell Nazi Symbols thereby hurting the sentiments of German people was significant for the jurisdiction[16]. In its initial ruling this trial court held that the U.S. website for Yahoo Inc. can be made answerable to French jurisdiction because it could be accessed from German people in France. The issues arose for its divergent legality existed in different jurisdictions. In USA, the sale of *Nazi* Items are protected under First Amendment. Where as in France such sales are prohibited under Article R 645-1 of the French Penal Code. These challenges of overlapping jurisdiction advances these complex questions: With the cross-border aspect of internet, is there any universal doctrines or theories that may prevail over and which court will have jurisdiction? How far any sovereign national government can assert the application of its laws and regulations to any Internet activities that has its primary activity originated from a different jurisdiction? Conventionally there exists three fold approach one as *Prescriptive jurisdiction* second as *Adjudicative jurisdiction* and the third as *Enforcement jurisdiction*.

[16] See:"*Yahoo! Inc.* v. *La Ligue Contre Le Racisme et L'Antisemitisme*, 145 F. Supp. 2d 1168, 1171 (N.D. Cal. 2001). In this case Yahoo Auctions, being one of the applications offered through the Service allowed its users to communicate through the use of the Service, to buy and sell items in an online auction, where Nazi memorabilia was also found as auction items."

Today when different parties and their nationalities are in question, there are certain presumptions pertaining to jurisdiction that the courts apply. In normal cases the court applies the general jurisdiction by applying the long-arm rule by stretching it over parties in other states to examine if the necessities in statute have been met and whether or not the application of jurisdiction would infringe the defendant's due process rights. In other words, a municipal court can exercise personal jurisdiction over a non-resident defendant-be it a company or corporation, only so long as there exist 'minimum contacts' between the other party and his or her nation State. When the court cannot apply general jurisdiction, the court will search for specific jurisdiction and accordingly it will be applied, for instance section 75 of the Information Technology Act deals with extraterritorial principle[17]. In the infamous incident of *Blue-whale challenge* as well, the effects doctrine was applied holding the administrator of a group or a community page responsible for their acts committed from one state or country, into another state's victim[18].

1.3. Curtailment to Right to Privacy

There exists a blurry line between the public and private sphere where one cannot state what constitutes public and private information. Also, with the unprecedented dissemination of information on social media websites there also lie the difficulties in defining sensitive personal information *vs*. Personal information, and this consistently has repercussions upon user's privacy. An enormous bulk of social networking sites fixed a certain privacy background as default so that everybody can view a person's record unless privacy settings are clearly altered. Information tracking mechanisms exist in many websites and advertising companies. Users' own favourites, behaviours and routine are easy to be pursued whenever a user log on to the internet he/she outrun a mechanized trail. This information is beneficial in corporate marketing especially in promotions that aim the individual customer. If a user logs on to any online shopping store for example myntra.com, then by default that user will get recommendations of such similar websites and in e-mail get hot offers from myntra.com. This condition leads to a rational conclusion that somewhere social networking sites are involving users' personal information for revenue purposes. Additional aspect of privacy infringement in social networks is the lasting accessibility of user's information to anyone. Even if user deletes the profile, the social media company still retains the data.

[17] *Karmanya Singh Sareen and Anr.* v. *Union of India* Writ Petition (C) No. 7663/2016] on 23.09.2016

[18] Rosenblatt B. Principles of Jurisdiction. Available at*:* http://cyber.law.harvard.edu/property99/domain/Betsy.html (accessed: 03.09.2019)

Safeguarding the privacy mandates isolation from unwanted publicity. This wish to embrace something personal often seems to be in clash with freedom of expression.

The frequent challenge between privacy and free speech thus fails to strike stability among the two competing interests". Therefore, at times, privacy is quoted as 'sweeping concept' by jurists and with the social media, there is no overarching conception of privacy. The jurisprudential principle on which privacy rights vest is often connoted as informational autonomy that implies the right to control the flow of information about oneself"[19]. However there are certain blurred areas where privacy right cannot be determined. For instance: (i) Can an individual in public space demand privacy? (ii) Can a public person demand for same privacy as any other infamous person? (iii) Can an exposed information be withdrawn in the name of privacy? (iv) Can privacy right be protected after the exposure of the private data? (v) Can truth be a defense in privacy right validation like defamation matters?

Thus it can be seen that the periphery of private or personal seems clouding and with technological advancement one cannot reasonable have privacy. Everyone's life is tracked and revealed. The argument in support of free speech would be sustained by the significance of the speech in terms of the public interest it serves."Accordingly, when personal information placed is watched in public space, human dignity is despoiled regardless of the public reaction to that information. It is therefore suggested that if the main aim is the right to privacy, revelation of private facts would be warranted only if it is outweighed or overridden by a public awareness in revelation [Birks P., 1997: 65].

The inspiration to provide readers with the most meticulous detail about the private lives of celebrities and public figures is definitely not a newsworthy information. Against this background, it is essential therefore that privacy law provides practical and effective protection if it is to respond to the examples cited above.

There can be a number of instances of privacy infringement in offline mode. Gazing at one's window at home that faces the dining table — In this window being a space to a room cannot be termed s public space. Same is the case with a car parked on road. Road may be a public space, but the car parked and the space within the car is private space. Gazing once by default and looking there several times to get any information are different. Listening to private conversations happening over the telephone is definitely an intrusion to privacy. It is for that reason the Supreme Court stated that phone tapping is a breach to privacy

[19] *See*, P. Regan. *Legislating Privacy: Technology, Social Values, and Public Policy.* University of North Carolina Press, 1995, p. 85–89.

right[20]. Similarly is the snooping at a profile in social media. The activities of a person that appear on newsfeed is different from being checked every time. These instances reveal that a there are certain moral conditions inevitable for invasion of privacy[21]. Privacy, as a result consists of access to an individual's information or any information concerning him [Rachels J., 1975: 323]. Every individual ought to disclose certain aspects of his private life and does not expect a loss of privacy on the ground that others gain access to him. If he chooses to allow himself any information to go public, then he cannot complain about privacy. But if he chooses not to allow others gaining access to his personal activities or information, any intrusion or a disclosure of his personal data would violate his right of privacy.

True that,"with the onset of web 2.0 and social media, individuals are facilitated to publish on computer networks without revealing their true identity. With the social media's unlimited search and memory capacity, even minute particulars of personal information can have a gigantic bearing, even years after they were shared or made public. It cannot be equalized to normal speech theories as to promote truth, political and social participation and self-fulfilment. Rather, this unauthorized access to personal information to large groups of people invites the harm.

Social media, in its original format, was not considered with privacy measures rather it was about divulging, involving, connecting, and access to information. With the *Camridge Analytica* exposure, it is felt that data about each of the users, held by third party stakeholders, is proliferating. The essential aspect informational privacy, in a world inundated in data, has become a matter of concern. The control over one's information as privacy is not a new origination that means limiting unrestrained usage of one's information -by protecting from undesirable usage of information about oneself. It is the skill to hold oneself -in the form of information — from unpredicted use of that information -such as by law enforcement, professional opponents, or even family members, characterized against or produced by marketers and others who classify all about oneself. This notion of safeguarding information about oneself from causing maltreatment is the main thrust behind core notions of privacy exemplified in the judicial clarification of privacy through various ground-breaking judgments.

1.4. Changing Privacy Policies and Setting

Many social media websites keep changing the policies and install new features in the websites without giving due notifications to the users. Social media web-

[20] *PUCL* v. *UOI* (1997) 1 SCC 301.

[21] Hong Kong Law Reform Commission, Consultation Paper on Stalking (Apr.,1998).

sites are the hub of collection of private user information that can infringe upon a user's privacy rights if no sufficient steps are taken while introducing new features. Many of these policies are highlighted only when user reads in the privacy settings or policy settings. There initially it was mentioned that the website owner obtains the rights to use and distribute the users' private information". Devoid of providing any reasonable notice, the terms of the exchange between the user and the social media website had been constantly changing and being presented with new features and services including the advertisements, Beacon[22], Newsfeed and Platform. This consequently has been leading to default modification in the privacy settings and the privacy policy. The algorithms and technology of social media drive the margins of disclosure—both voluntary and involuntary—along with privacy policy in the terms and condition. With the emerging trend to log in to all social media websites and apps with websites also letting the sites to access the data results in invasion to privacy [Gavison R., 1980: 421].

With the changing realms of the public and private and considering those as relative terms and shift according to individual perspectives, defining the privacy policies in social media platform is difficult. Additionally there is no supervisory system as it works under the principle of self-regulation. Necessary to have privacy is not about trying something to hide. It is about calling for safeguarding the control of one self. This is the self-regulatory regime with definite policies. Thus can be seen that many of these issues deal with the questions of: (a) Whether the effect by way of harm is to happen to create safeguard for infringement of privacy? (b) Whether 'private' refers to a category distinct from confidential? and (c) Whether privacy revelations have any safeguard under right to freedom of expression? It is the need of the hour to view privacy as protecting one's identity. By safeguarding against revelation of the information, the discrimination can be prevented, providing a kind of remedy in anticipation of the harm[23]".

1.5. Identity Theft

Identity theft is when a person fraudulently attains and operates in someone else's character. Thereby one 'appropriates' another's identity and uses it without consent. From social media, once the network circle is understood, spamming and phishing are done and thereby spam emails are composed to potential targets.

[22] Hashemi Y. Facebook's Privacy Policy and Its Third-Party Partnerships Lucrativity and Liability. *Boston University Journal of Science*, 2009, no 15, p. 159.

[23] Prominent privacy scholar Anita Allen suggests that there has been the rapid erosion of expectations of personal privacy **...** people expect increasingly little physical, informational, and proprietary privacy, and **...** prefer less of these types of privacy relative to other goods. See generally Allen A. Coercing Privacy. *Wm. & Mary L. Rev*. 1999, vol. 40, p. 729–730.

The emails composed in such manner randomly avail information such as Social Security Number, bank account details, etc. Social media seek such information that can identify users and its privacy settings allows users to select how the information can be used. Users have the choice to take in location information with their posts which will be stored to provide features for services. Once user gives the location and geographical place, then user will start receive new trends, stories, ads and suggestions for people to follow. Such feeds are helpful for the perpetrators to do identity theft and do the transactions through social media with spamming and the phishing.

1.6. User Tracking and Cookie

'Cookie' is a term developed from HTTP cookies to track the general visitors to website in order to trace how often the persons visit were developed so a site could generally identify a visitor and keep track of how many times one visited the website. They are minutes of data stockpiled in browsers. Such information had been used for direct promotion programmes that target the individual customer. Such general information collection soon advanced as the past browsing behaviour of the visitors' within a site, and also use the personal information willingly provided while registering for the content. Currently, it is a general trend for most of the websites and advertising companies to track user as he or she leaves behind an electronic trail. For instance, if one individual visits a website, the website via cookie acknowledges that individual as user A. If that person leaves the site and then browse the site once more, the cookie information stored in the website will recognize that A is the same user who was browsing the site previously. The area of concern is when an unapproved website uses any user/visitors details for proxy and initiates attack by conferring fabricated gathering of data to and take up the user's activity. Many social media have acknowledged the prevalence of cookies in their websites. Additional part of privacy infringement in social media is the permanent obtainability of any user's information to other users. Many social media servers have permanently keep the user account even though the user deletes complete information of account.

1.7. Default Search Result

"Initially the users' profiles were openly available as default search by non-user on many social media. By this, anyone not being on social media could also trace 'users' names, profile photos, address book, list of friends and even the pages which they are member in or even the places they checked in and so on. However with various criticisms from all over the world, they did change the settings. Even

then there are various social media such as *Linkedin*, *Google Plus*, *Academia.edu. in* where users' profiles are traceable with public search option."The arguments debunking the privacy on FB revolve around the rationale that users key-in the information, and it is a social networking site, hence users waive of their privacy by taking part in such networking and being a part of social media". To address this, the best case judgment would be of *Y.G. v. Jewish Hospital of St. Louis*[24], a couple incapable to conceive a child endured *in vitro* fertilization at the opposite party hospital. The process was effective however they had decided to keep it confidential for personal reasons like- disclosing their involvement would affect the religiously-especially when church condemned the practice. Hence only the hospital authorities and their very near relatives knew of the couple's participation in the *in vitro* program. However, the issues cropped up when the couple was invited by the hospital's successful fertility programme for which they got clicked by a camera crew. After the transmission of this program, the couple was traced and they stated that media breached their privacy right. The question was if any reasonable foreseeability existed for their breach of privacy? The court disallowed this contention, holding that being present in the party within hospital invitees clearly meant that the couple chose to disclose their involvement to only the other *in vitro* couples. This case is an example of stating that privacy right and letting the information go out of one's hand is not within the concerned person's limit. How much ever precautions one takes, certain information may go out of reach and in such case the other party has to be made liable.

1.8. Anonymity

The prevalence of anonymity in onsite medium is occasionally applauded for it enhancing the freedom of online communication. Anonymity however gives perpetrators opportunities to commit unwanted activities under the mask. Anonymity revitalises embarrassments and can lead to uncommon doings thereby it can lead to misbehaviour, for instance harsh or rude language and acts that are critical or dangerous. With each computer portal to the web holding a unique Internet Protocol (IP) address that is logged every time a user visits a website, one's anonymity is nearly always traceable. However certain damages caused by anonymous user can be irretrievable. Anonymous services are often taken as advantageous by perpetrators and that can affect safety and security at large. If activities are done in idiosyncratic or outwardly performed for fun or amusement, it should not be tracked. But the kind of communal, hate messages or misinformation generated by anonymous profiles are detrimental in nature.

[24] 795 S.W.2d at 502.

"Currently, under the civil litigation, the legal system provides for a remedy in lawsuit and it is known as a *John Doe* lawsuit. Under this the complainant can lodge the plaint by suing an"unknown defendant."The best example of anonymity is the case of Rahul Pashupal and his wife Reshmi for launching the webpage and Facebook by label *Kochusundarikal* depicting pornographic images of minor girls along with others, with abusive and sexual comments and made wide circulation in social network and made advertisements through the Internet[25]. There are reports that assert that marriages of women victims were blocked due to their online victimization[26]. However many women at this instance choose to endure these pains without reporting petrified of social stigma[27]. When cyber-crime strikes, persons take it individually and essentially blame themselves for some cases of cyber-crime. Even when it comes to online pestering or being approached by a sexual predator, some victims yet blame themselves. There are certain profiles creates by anonymous people and track certain people and to find the whereabouts. There are cases reported where thieves see a status update of a family being on holiday for a lengthy period of time and jump at the perfect opportunity to steal some valuables."

1.9. Cyber Bullying and Trolls

In India, there is IT Act of 2000, amended in 2008 that deals with cyber bullying under Section 67. However there are certain loopholes, especially when bullying has become rampant among school going teenagers. Targeting a person and harassing and embarrassing to negative, aggressive, and mean-spirited objectives are condemned for the repercussions it will have. With the prevalence of social media, the creation of web-page within social networking sites depicting pornographic pictures of minor children, with abusive and sexual comments and was circulated among the public widely is also widespread. Additionally, social media facilitated the rising number of bullying. There are various cases reported about bullying. The social-media page or web-links are created by student-administrators by name confessions are increasingly reported as bullying platform[28]. Apparently various colleges, schools with batch division number have these confession pages. The ac-

[25] *See* Crime No. 34/2015 of Cyber Crime (Case against Rahul Pasupal procuring the minor girls for the purpose of sexual abuse and was a part of a racket involved in the trafficking of minor girls for sexual abuse having wide B.A.Nos.866 of 2016 and 867 of 2016 2 spread roots through out Kerala and even outside.)

[26] *See* J. Finn & M. Banach. Victimization online: The downside of seeking human services for women on the internet. *Cyber Psychology & Behaviour,* 2000*, no 3,* p. 785–796.

[27] Human Rights Watch,'Events of 2018' Available at: https://www.hrw.org/world-report/ 2019/ country-chapters/india (accessed: 22.05.2019)

[28] Gowri M. Confessions or Cyber-Bullying. *The Hindu*. 4 July 2013.

cess and admittance is possible with administrator who stays anonymous when grant the entry pass to the requested ones. Given the fact that candid comments enthuse the group, the members promote such confessions. The outburst of such emotions can vary from experiencing feelings of resentment, hurt, humiliation and anxiety. These emotions can cause teenagers to adults to pursue vengeance on the bully, to pull out into themselves or even commit suicide[29]. This is sort of bullying for the targeted person. User publishing personal information on social media pages is inclined to bullying for the disclosure of information that is kept private in real lives. The easiness to generate fake profiles again provide an occasion to state anything about another individual without the apprehension of any outcomes. This is corresponding to online hostility and cyber nuisance.

Whereas trolling is another way of targeting celebrities and politicians for their embarrassing statements or funny moments or their public appearances or statements. It can be humorous however it is characterized as an irregular behaviour with destructive bearings on online communities. Trolling has been drawing attention after social media as it generates provocation to absurdity. Trolling is contextual and cannot encompass all its behaviours. Compared to the traditional forms of bullying trolling cannot be identified for the mass generation of it by trollers and that it occurs 24 hours a day, 7 days a week and are shared like viral ones. It can also have a far reaching effect for the videos and posts being shared across social networking sites can be seen by large audiences. Cyber bullying is a modern version of until then prevailing conventional offline bullying. The difference is that under cyber bullying with bullies are not known to the victim. Trolling is done by anonymous group who are totally unrelated to targeted ones. This fails the police and the authorities to keep stride with progressing technology and the voidness in current laws to report the matter to be investigated upon.

1.10. Cyber Stalking

Stalking until causing harassment is unknown since most of the social media do not publish who visited profile list". Even if such list is published to the user who wants to know who all have seen his or her profile, that cannot be called as stalking since the purpose of such profile is social connection and for the very purpose people have to see, view and search for people they know. It is pertinent here to state on *Ritu Kohli* Case[30], being India's first case of cyber stalking. Though these are offences under Information Technology Act under 67 A, 67 B of the IT act as

[29] Cyber Laws Compendium on Bullying. Available at: https://cyberbullying.org/bullying-laws (accessed: 08.08.2018)

[30] Orkut Community rules. Available at: http://www.worldpulse.com/en/community/users/mukut/posts/22772 (accessed: 02.11.2018)

blackmailing, cyber-bullying, Cyber stalking or harassing, sending obscene messages through any electronic mails, not much developments ensuring the safety of women and children happened so far. Additionally, there could be intimidations of physical or sexual vehemence by email that degrades her identity and other traits (for instance sexual orientation).

1.11. Standard Contract and One-Sided Terms of Service

The terms in a contract are termed as standard when they are not premeditated to negotiate the interests of opposite party/ies rather take one way encompassing the interests of infinite customers[31]. Indeed, with the e-commerce transactions and boom of C2C, B2B, B2C *etc*, the users have no choice but to get into a social media site. From the earlier notion of consumers as king, today it has moved to consumer in need of goods or services and that gave corporate giants to control consumers. The users who want to be members in social media lack the bargaining power and thereby they lack the power to negotiate or modify the terms of the contract. Even then, the standard form of contract is preferred for it supports competence in contract law, which saves time and negotiation charges.

The enormous volumes of data (for instance uploaded pictures or video slides) in the clutches of the social media have been agreed to be used by the terms and conditions they put forward by way of standard form of contract. The user's categorical and blind approval of social media terms of Use and further users' disclosure of information about themselves in order to be able to interact with other people are increasing their venture, obligation and confidence in the social media itself. This means users do not only have an association with other users but also with the social media itself, which gains strength as the users get more involved in it.

As put forward by Aaron Chiu, As long as the site is dominant and competitors remain far from the tipping point, it can dictate the terms by which users will be bound [Eisenberg M., 1982: 741].

This issue of unconscionability had been tested by judiciary in various cases on the grounds of unequal bargaining power and substantive unfairness. But it had been held that:"…unequal bargaining positions, undue length, fine print, confusing language, and misleading terms, or the fact that a contract is a standard form

[31] Neumayer K. Contracting Subject to Standard terms and conditions. *International Encyclopedia of Comparative Law*, vol. 6, 1999, p. 12–17. The author states: "As social media users, our rights are established through non-negotiable, one sided and deliberately opaque 'terms of service' contracts. These documents are not designed to protect us. They are drafted by corporations, for corporations. There are few protections for the users-the lifeblood powering social media".

agreement, or contract of adhesion is nebulous concept...however they are enforceable unless the substantive terms are also unconscionable

"The grey area here is whether that consent is adequate. It is governed by the self-regulatory regime of contracts between the social media site and the user via the site's privacy policy. However the basic test of unconscionability of a contract remains the same. It is to find out:

"whether the clauses involved are so one-sided and it gives no scope of compromise"

"If it aims to oppress or unfairly give a setback upon the other party?"

"These clauses thus are analysed taking into account the conditions that were present at time of making of contract, overall commercial circumstances and the facts and situation of the particular case[32]".

1.12. Information Mining

Social media websites write in their policy their policy vaguely stating that they do information mining. Many companies for their business purposes use data mining algorithms, implanted in bigger knowledge discovery procedures and systems, are programmed analytical tools that have lately practised a speedy surge in use. Social media has facilitated users to generate unimaginable amounts of structured and unstructured data. The arena of data mining is attaining implication appreciation to the accessibility of large amounts of data, effortlessly composed and stored via computer systems. With the prevalent and endless assortment of information about persons from manifold sources, many data brokers are equipped identify user characteristics and certain inclinations without having any information conventionally considered personally identifiable information. When these data are amalgamated and extracted, they can deduce a person's choices, connections, information on finance, address, usage of bank transaction, insurance, medical records, and political interests. There are apprehensions that with the accumulative level of storing of private information there is a larger danger that unsafe or even derogatory practices might be generated.

1.13. Use of Third-Party Apps on Social Media

From what it had been visualised, many social media websites had expanded into an abundant giant information source with users their friends and various pages, communities, occasions, and group pages many personal data and interac-

[32] Facebook Principles. Available at: http://www.facebook.com/principles.php (accessed: 20.06.2019)

tion information. Thus gradually social media is presented by the large quantity of information communication between third-party developers and users itself. When social media offers applications –Apps- initiated by third party application providers, it provides access to users' personal information via installed Apps. This admittance happen outside the loop of communal conviction with the user not being attentive whether anyone had installed the App collecting any data.

Various studies show that many unsecured social media profiles and apps do a hacker's work by collecting details. They can study who the top people in an organisation are to be targeted at to gain information and thereby to start phishing attacks or learn employee job roles, addresses and contact information [Eisenberg M., 1979: 67]. That's the reason why the third-party apps permission to gain access to an individual's profile including their contacts are often difficult to verify. Additionally there are no set rules or regulations for app developer to follow when it is provided to a greater platform for usage. The platforms like Google or Android or Apple have their own developer program policies, along with the developer distribution agreement. With the growing concerns over customer data many platform calls for regulations that increase transparency with regards to how apps make use of customer data. By way of developer license agreement a clause is added so that developers will be accountable the way they handle user data. Google recently modified its regulation in line with European Union's GDPR and it calls for more clarity regarding usage of data from how they amass it to what it might be used for is available to all users. In his testimony before the US Senate post *Cambridge Analytica* exposure, Facebook CEO stated that there is a prospective legal risk connected with social engineering and hoaxing outbreaks against users and the magnitudes of leakage because of app developers as a result of social media is irrepressible.

1.14. Memes

"Undoubtedly, social networking sites proffer individuals both with a vibrant forum for self-expression and with a platform for concerning to an extensive array of speech in society at large. Memes are usually hilarious representation or image of some incident. Initiated as advertising slogans, its usage and diffusion provide a speedy and active way of generating interest. However some can turn out to be sarcastic and defaming. Comical memes are also shared purely for fun which provides some one-line dialogue from cinemas and re-count it to the taken notions and situations. Another issue is copyright violation. Simply retweeting someone else's memes can possibly be generating a legal action. In legal footings, it is a 'derivative work' and merely the copyright owner has the legal claim to generate such work. Even though the individual claims to have made a fair use of the copy-

righted work, it can be used as a defense under the requirements of the Copyright Act. If any legal issue crops up with memes sharing and re-sharing, it can land up trouble to those who have re-shared the same. In USA, Warner Bros were sued under infringement of copyright after they being found using the famous 'Nyan Cat' and 'Keyboard Cat' in their game *Scribblenauts Unlimited* [Swirsky E., Hoop G. et al, 2014: 60–61]. Some memes are so mean that it generates a lot of distress and injurious consequences to the targeted victims.

1.15. Evidence Submission From Social Media

"Social networks are with time becoming a source for the discovery and search of criminal activity by members. Information concerning to a user's social media page can be accepted as evidence in the court of law. A glaring example is the case where police had to investigate on the stolen goods where a woman was suspect. The police in such cases look for her profile then went onto examine her posts, activity streams, status updates, messages and happened to see her update regarding display of goods she had shoplifted[33]. Social media profiles is decisive to know the identity of especially to spot the location of the executor of a crime."

"Evidence from social media websites, commercial websites, and private and employer-owned e-mail accounts are used for both civil and criminal matters. In discovery requests, this electronic content often included, and courts generally apply the similar paper discovery rules to electronic discovery. Social media content, even though posted or created private, is not shielded from discovery. For the larger interests of society and to maintain equity, evidences can be brought forth no matter how and in what scenario the related evidences are used by the culprit. In *Giacchetto* case, the Federal Court of New York stated[34]": "A party to an action can request a protective order to limit the scope of discoverable information and can sometimes include a 'pull back' stipulation or court order in which the party can call back a privileged document that was inadvertently produced during a discovery request"

Due to the prevalence of 'hacking' in social media accounts — whereby an unapproved user accesses other user's account — it could create a chance for reasonable repudiation concerning any specific instance of generated account. If authenticity of produced document is contested, its legitimacy has to be established and ensure that the evidence has not been tampered. The other issues involve when individuals often have countless social media and email accounts, in which they may or may not use their actual names.

[33] *Romano* v. *Steelcase, Inc.*, 907 N.Y.S.2d 650.

[34] *Giacchetto* v. *Patchogue-Medford Union Free Sch. Dist.*, 293 F.R.D. 112 (EDNY2013).

2. Duties and Responsibilities of Information possessor or Carrier *vis a vis* Intermediary performing dissemination responsibilities

As per the common law jurisprudence, if there exists a contractual relationship, any sort of contravention of confidentiality is considered to be a breaking of contract and hence the infringer will be liable for damages. There are certain scenarios where despite having a contract, for the relation or fiduciary relation that exists with the parties, such confidentiality is implicit. There comes a responsibility not to disclose confidential information, even though such a responsibility is not mentioned in the provisos of the contract. Any such breach can result in a legal action for damages endure due to division of the confidential information and also an injunction to hold down the further spread of the confidential information. In the case judgment of "*Saltman Engineering Co Ltd. & Others* v *Campbell Engineering Co Ltd.*[35] the court held that the responsibility to maintain confidentiality exist even in the absence of a contract. In social media with the people having multi-facted connections when get into dissemination. These issues above mentioned once again reiterate that within traditional speech doctrine, different types of media are given different possibilities of protection and deference with respect to content control. On one end of the scale, newspapers are provided with great extent of editorial choice in deciding upon what content they should distribute. On the other end, telephone companies-categorised as common carriers-cannot standardise the content that traverse their lines. Cable, broadcast and other media are positioned between these two limits and obtain some amount of flexible mechanism. Social media having the traces of media how far is the information carrier is the dispute especially when vast amount of data and information are disseminated. Media as information carrier, it signifies the conventional concept of the press clause as defending all news media (from non-news media) which carry out a recognized and valued function in assembling, editing and disseminating information to the public. Secondly, it indicates an independent role for media not merely restricted to information-gathering period but also to the editing/scrutiny or the publication process or dissemination stage. By this it mandates to distinguish between 'publishers', 'disseminators' and other speakers in this regard.

The term 'dissemination' in its literal sense means spreading ideas or information by propagation[36]. Under Art. 10 of the European Convention on Human Rights (ECHR) 193, media is made accountable in imparting accurate information

[35] [1948] 65 RPC 203. Available at: https://www.jade.world/cases/19633AllER413 (accessed: 03.12.2020)

[36] Li T. Beyond Intermediary Liability: The Future of Information. *Yale law Journal*, 2018, vol. 52, p. 129.

to public[37]. By ratifying this Convention, all the nation-states have had an 'affirmative duty' to grant independence to the editorial staff of newspapers. This is unlike a common right of access to newspapers assuring the publication of everybody's information or ideas, whether in the form of articles, opinions or comments. That differentiates free speech and free press under every Constitution of democratic nations[38]. Freedom to impart is here of a more responsible task since Art. 10 of ECHR provides that a state may require the licensing of 'broadcasting' audio or visual media. Their publication depends on the private publisher's or Editor's free decision. By this, usage by any private citizen or organization to have access to broadcasting, unlike freedom of speech, is limited. Simultaneously it guarantees media to have a core set of skilled professionals safeguards that news production standards are inordinate and that extensively held ethical values are followed.

"The concept of reporters' privilege is not of contemporary vintage. Generally, these *de facto* protections from common law have played a critical role in shielding the press and preserving the flow of information to the public. This conferment of privilege keeps apart publishers from speakers for the responsibility they have. The goal of the privilege is to nurture whistle-blowing and other lawful revelations. As in all privilege situations, a potential of confidentiality should be assumed and it is to be tested to the degree permissible by law"[39]. Law confers the privilege to journalists or reporters in mainstream media as qualified privilege where the information if found fair, accurate and not actuated by malice[40]. Thus it needs to strike the right balance on[41]: (1) How much of this communication is vital to society; (2) In the absence of a privilege, if such communication will be inhibited; and (3) The cost to the legal system by losing access to the privileged information. To get privilege, it needs to be shown that the concerned entity or person has been in

[37] Art.10, European Convention on Human Rights (ECHR) 1953 states: …Public broadcasting services have to be protected by the freedom of expression. Freedom of press forecloses the state from assuming a guardianship of public mind. That watchdog approach helps in discovering the truth to people at large who can thus form opinions

[38] Press clause and Speech clause are the dual clauses implicit in Article 19 (1) (a) of Indian Constitution.

[39] Zampa J. Journalist's Privilege: When Deprivation Is a Benefit. *Yale Law Journal*, 1999, vol. 108, p. 1435. The author states: …Common law confers the privilege to journalists in terms ofthe social institution in which they operate and the democratic functions that they provide for society…"

[40] See Section 499 of Indian Penal Code, 1860 with the Exceptions provided.

[41] In the US judgment of *Reporters Com.* v. *American Tel & Tel*, it was held that there has to be three minimal tests conducted: That there is a reason likely to consider that the reporter holds information which is clearly related to a definite possible abuse of law. That the information it pursues cannot be gained by alternate ways, which is to say, from sources other than the reporter. That there includes an interesting and superseding interest in the information. See *Reporters Com.* v. *American Tel & Tel*, 593 F.2d at page 1039.

journalistic work of reporting or dissemination or circulation of information under public interest to impart newsworthy information to public. This conferment of privilege is on the basis of what dynamic, robust and active role news media journalists play in imparting information. For instance, newspaper delivery boy cannot be made liable for any information in the form of new paper he is delivering to people. How can a librarian be made liable for any contents of the books he is taken care of in library? These are the passive roles — often equated like *Postman rule* — are for carriers of information who is not aware of contents.

Here a categorical distinction is to be made between Information owner, Information possessor or holder, Information Disseminator or Information Carrier. The distinction is important in terms of conferring this Media as a watchdog has its distinct responsibilities and it can be carried out with the privileges or immunities provided by State. Qualified privilege at Common law applies where communications take place for honest purposes, and, therefore, this privilege can be defeated by malice. Such qualified privilege arises on occasions where there is a legal, moral or social duty to publish the information in question or when the person who receives the information has an interest in receiving it. It does not matter if the information given turns out to be untrue, provided that the statement was not made with malice[42]. Journalist-source privilege is termed as qualified privilege for the responsible task he performs. The"goal of most legal privileges is to promote open communication in circumstances in which society wants to encourage such communication [McCullough C., 2014: 176].

"For this reason, in social media, though people are self-content providers and self- editors and self- disseminators", they cannot call themselves like a reporter or editor or mainstream media persona for the lack of accountability journalism [Alexander T., 2017: 612].

Mainstream media whose main task was to gather, identify, edit and report the news has thus a qualified privilege in opposition to disclosure of any information, documents, or items obtained or prepared in the gathering or dissemination of news in any judicial, legislative, or administrative proceeding in which the compelled disclosure is sought. Unlike this, Social media provide multitude of services such as access to the platform, letting users to amass and publish content, do marketing and advertisements related work, to post photos, videos any documents etc."It is the medium amongst a person and the internet, letting them to upload, share or disseminate the content in any format. When users involve in internet shopping they do not use 'media' in its normal sense. The content and posts submitted by users are not verified or moderated, not edited or amended.

[42] *See* Smith D. *A Theory of Shield Laws: Journalists, their Sources, and Popular Constitutionalism*. LFB Scholarly Press, 2013, p. 252–255."

People express themselves without the help of an editor posting their contents. Social media gives everybody the occasion to circulate individually whatever they like."There are no stringent limitations on format, access, or contents. This leads to the conclusion that the social media is not a mainstream media as it was understood. They are using a 'medium' — a mediator for their activities.

Paradoxically, it does not recognize the content of the *cache*, nor do they are aware the content of the hosted material. This service as internationally termed as hosting service only diffuse the content that their 'customers' have submitted distinct from"a newspaper editorial office, which receive articles and reassess them and edits them individually before publishing, these sites."Therefore, hosting providers globally are not held liable for information for no actual knowledge of any unlawful activity or information if happens within the platform. In addition, upon obtaining such knowledge they have to expediently remove or disable access to the information. Many judgments had been rendered in this line that if the recipient of the service (the content provider) was acting under the control of the hosting service provider, the latter cannot be exempted[43]. Public policy positively encourages the proposal that individuals who have information of noteworthy value should normally be supported to express that information to the society. Society would want to promote the communication, and without a privilege the communication will regularly be chilled. Hence extending the legal right, privileges and immunities to social media is not constitutionally valid and that will result in irreparable harms to State, society and people at large. These raise the questions as to : If the people have a right to know, what is it that they have a right to know and who has the correlative duty to provide what the public has a right to know? Is the right to know a fundamental right derived directly from the Constitution, or is it a right that stems from a broader societal goal? These questions suggest that certain limits within the social media exist that cannot be made applicable to media. When people are posting the so-called news, there exists these issues on what to be posted and what not to be posted. And once the so-called information is posted, it cannot be called back. The affected parties can challenge only if the posted information is false. If the information is true and it ought not have published, there exists a moral right not to publicize everything. This is a dark area when there are certain information that cannot be shared or circulated for its pertinence to notions of personal autonomy and privacy. This means there exists certain unwarranted disclosure of information that might affect people at large. Those who uphold that there is a constitutional right to know, or that there ought to be, would define the concept as a right to receive information or communication and the right to ac-

[43] In the judgment — it was held that hold hosting service provider cannot be made liable if it did not: (a) Initiate the transmission; (b) Select the receiver of the transmission; and (c) Select or modify the information contained in the transmission.

quire or gather information. The latter notion has been argued as justifying a right to keep one's sources of information confidential. Privileges are granted by law to guard the content of confidential communications made throughout a privileged association. By this, the communication may not be admitted into evidence if the privilege is correctly emphasized by the person who made the communication.

Having observed the summary of Justice B.N. Srikrishna Committee report on Data Privacy and Personal Data Protection Bill, 2018, also considering the functioning of Indian polity balancing both — a vertical federal structure along with horizontal working with three organs of government structure"- imbibing the separation of powers, there is a necessity to have a legislation dealing with the way people's data is collected, utilized and shared by corporate companies. For this there is a need to divide the data as general data and highly sensitive data. Though under section 43 of IT Act, 2008 has provision to hold a corporate body accountable if any recklessness comes in handling data happens, or not creating reasonable rules on data processing, what all can come under sensitive personal data is still a dilemma. There is a need thus to lay down various conditions such as consent requirement", legitimate purpose", purpose limitation", succeeding withdrawal of consent etc. to inflict on the body corporate while amassing any such information. There is a lacuna currently on Rules require the prior consent of the provider of the information while disclosing sensitive" personal data to a third party. Consequently, a crucial foundation for processing of personal data is the individual consent that mandated the necessity to have a proper consent formation. Neither the consent be made uninformed nor momentous rather it functions in an all-or nothing fashion."

Another finding of the report was that — data flows in India is a consequence of a simplistic assumption that data flows are an unadulterated good", hence the data flow happening within and outside Indian jurisdiction can cause substantial damage. This provides an unlike character to the expression in various jurisdictions choosing the person whose data is being amassed as the data subject and the body that assemble the data as the data controller". This arises from an assumption that the association involving the individual and bodies with whom the individual distribute the personal data is one that is based on a primary expectation of faith. In spite of any contractual association, an individual suppose that the personal data will be applied reasonably, in a mode that accomplish necessary significance and is logically estimated. This is the trademark of a fiduciary association. Pursuant to this, conditional on the temperament of data that is collected, the rationale behind such collection, the bodies with which involvement do take place, data principals envisage shifting degree of reliance and reliability. For bodies, this deciphers to an obligation of care to cope with such data reasonably and dependably accepted by the Principals and therefore it could be called as data fiduciaries". On

this basis the proposal of the Committee was that such flows cannot be unencumbered, and definite responsibilities need to be forced on data fiduciaries who yearn to reassign personal data beyond India. At the same time India's national interests may require local storage and processing of personal data with obligations on data fiduciaries and rights of data principals. Anyone who uses personal data has an obligation to use it fairly and responsibly. This is the cardinal tenet of the proposed framework.

This approach will safeguard individual autonomy plus privacy which can be attained within the facets of an open and reasonable digital economy. At the same time, in lieu of legitimate interests of state as provided under Justice *Puttaswamy* Judgment[44], there may be instances where rights and obligations of data principals and data fiduciaries do not affect in entirety. This manifests in limited instances where consent may not be used for processing to serve a larger public interest such as national security", prevention and investigation of crime", allocation of resources for human development", protection of the revenue"[45]. "However, on the right to be forgotten,"the Bill notes that 'data principal' which means the individual or the person providing their data, has a right to right to restrict or prevent continuing disclosure.""But the bill does not allow for a right of total erasure like the European Union does. Another highlight is that the bill mentioning about handling of "anonymisation proportionate to personal data, wherein it proposed that the irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified, meeting the standards specified by the Authority.

Conclusion

Social media rely on information that tend to soften privacy concerns, signifying that the information is voluntarily (though users have no choice) submitted by users. Social media creates a new generation of audience-producers and this hazes the central line amongst access to the means of online content production and ownership or control over these resources where privacy is at stake! It has been observed that by the virtue of liberty, freedom and right, every human being has the right to communicate his or her opinions and ideas and share information in whatever form in accordance with legal parameters. The freedom of speech and expression has various facets and one among it, the freedom of press is a public service with a duty to the people[46]. The open course of information, which is so

[44] *K.S. Puttaswamy(Retd) v Union Of India 2017 (10) SCALE 1.*

[45] See BN Srikrishna Committee. *Report on Data Protection Framework*. June 2018.

[46] Arun C. Making Choices: Social Media Platforms and Freedom of Expression Norms in: L.

necessary to effectual self-governance, is considerably important with the subsistence of a free and robust press. For this, the press must occupy in numerous precise positions and display some unique features. Since they are viewed as so essential to a flourishing and vigorous democracy, these desirable position and features have progressed into a set of debates concerning the media.

The degree at which exchange of communication existed had been multi-folded with sudden increase in information collected and circulated. Today every news-media has its social media web page including *Twitter* handles or *Facebook* pages thus stories are searched on internet service providers to know if any user has uploaded anything that became 'viral'. Moreover, it has become a necessity for mainstream print media to have their websites, live videos, journalists' blogs, invited newsrooms debates where invitation is extended to community participation. The bloggers consider themselves as journalists and break *scoops* and stories. With the notable shift to mobile news access news has now become omnipresent-available on every platform at any time."Regardless of their professions, resources or training today, *netizens* are disseminating news to the public themselves. Personalized and participatory stories having maximum views or shares are now converted as news. In a democratic country, news should be based on what the people need to know not on what the public wants to know. This upsurge in 'citizen/selfie- journalism', through social media is jurisprudentially affecting the information matrix and constitutionally envisaged rights and freedom.

References

Alexander T. (2017) Social Media Accountability for Terrorist Propaganda. *Fordham Law Review,* vol. 86, pp. 612–615.

Bill J. (1972) Class Analysis and the Dialectics of Modernization in the Middle East. *International Journal of Middle East Studies*, no 3, pp. 417–434.

Birkinshaw P. (1988) *Freedom of information, law, practice and ideal.* L.: Weidenfeld and Nicolson, pp. 140–146.

Blanchard M. (1986) *Exporting the First Amendment: Press-Government Crusade of 1945-1952*. N.Y.: Longman, pp. 34–38.

Brownlee J. (2019) Low Tide after Third Wave: Exploring Politics under Authoritarianism. *Comparative Politics,* vol. 34*,* pp. 477–498.

Chiu A. (2011) Irrationally Bound: Terms of Use Licenses and the Breakdown of Consumer Rationality in the Market for Social Network Sites."*South California Interdisc Law Journal,* vol. 21, pp. 167–213.

Bollinger and A. Callamard (ed.) *Regardless of Frontiers? Freedom of Expression and Information in the 21st Century.* N.Y.: Columbia University Press, 2019, p. 382–383.

De Sola P. (1983) *Technologies of Freedom*. Wash.: Belknap Press, p. 76.

Donath J., Boyd D. (2004) Public displays of connection. *BT Technology Journal*, no 1, pp. 71–82.

Finn J., Banach M. (2000) Victimization online: The downside of seeking human services for women on the internet. *Cyber Psychology & Behavior, no* 3, pp. 785–796.

Franklin B. (1737) Freedom of Speech and Press. *Pennsylvania Gazette*. November 17.

Hackworth B. (2011) Are Consumers Following Retailers to Social Networks. *Academy of Marketing Studies Journal*, no 5, pp. 1–23.

Knutson A. (2009) Proceed with Caution: How Digital Archives Have Been Left in the Dark. *Berkeley Technology Law Journal*, vol. 24, pp. 437–474.

McDermott K. (1982) Liability for Negligent Dissemination of Product Information: A Proposal for Assuring a More Responsible Writership. *Forum,* no 18, p. 557.

McPeak A. (2015) Social Media, Smart phone, and Proportional Privacy in Civil Discovery. *University of Kansas Law Review*, no 1, pp. 235–292.

Mill J.S. (1964) *Representative Government*. L.: Everyman's Library, pp. 26–28.

Moore P., Salloukh B. (2017) Struggles under Authoritarianism: Regimes, States, and Professional Associations in the Arab World. *International Journal of Middle East Studies,* vol. 39, pp. 47–70.

O'Reilly T. (2007) What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software. *Comm. & Strategies,* vol. 65, pp. 18–19.

Smolla R. (1992) *Free Speech in an Open Society*. N.Y.: Knopf, pp. 271–277.

Stacy A. (2017) Paying for Privacy and Personal Data Economy. *Columbia Law Review,* no 6, pp. 1375–1376.

Ten C. (1969) Mill Liberty. *Journal of the History of Ideas, no 30,* pp. 47–68.

Van Niekerk B., Maharaj M. et al (2013) Social Media and Information Conflict. *International Journal of Communication*, no 7, pp. 1162–1184.

Wacks R. (1989) *Personal Information: Privacy and the Law*. Oxford: Clarendon Press, p. 432.

Yigit F., Tarman B. (2013) Impact of Social Media on Globalization, Democratization and Participative Citizenship. *Journal of Social Science Education,* no 1, pp. 75–80.

Zhu J. (2009) Roadblock and roadmap: Circumventing press censorship in China in the new media dimension. *University of La Verne Law Review,* vol. 30, p. 404.