CHAPTER 2

REGULATORY CHALLENGES BEFORE SOCIAL MEDIA

The greatest gift to mankind from the scientific community has been the invention of information technology and the associated communication technologies in the last decade of the 20th century. This technology is of such monumental importance that it has been rightly termed as InfoTech revolution. These technologies have put entire human civilization on a fast forward mode by introducing unprecedented speed in information & communication via social media. Social media in particular has greatly impacted political dynamics on a global scale by enabling users to express themselves publicly in ways previously unavailable to them. This very shift in communicative power has spawned greater efforts to restrict and control the use of the internet for information and communication on political, moral, cultural, security and other grounds. This effort of controlling the internet has led to legal and regulatory initiatives to mitigate risks associated with this new medium, ranging from privacy of users, intellectual property, national security, to frauds, pornography and hacking. Regulatory challenges of social media can be broadly addressed under two heads namely

- Legal Regulation
- Moral and Ethical Regulation in the form of guidelines by various statutory authorities like election commission.

The chapter heavily focuses on legal regulatory regime, which constitutes the bulk of regulation in India & other legal systems. It identifies the various problems generated by social media. The chapter also critically analyzes the relevant laws and functioning of regulatory authorities in addressing of these problems. An additional narrative discusses the moral and ethical guidelines for regulating the social media.

---

38 Ajay Yadav, ‘The Legal Complexities of The Digital World’ (2012) 18 Lex Witness 1

39 Wolfgang Danspeckgruber ‘Introduction’ in Princeton University (eds.), ‘Social Media Revolutions: All Hype or New Reality?’ (Spring, 2011)

2.1 PROBLEMSPOSED BY SOCIAL MEDIA

The basic architecture of social media platforms provide unique opportunity of interaction to the common masses, which have resulted in great problems to the society. The overthrow of autocracy in Arab world (mainly Egypt, Libya and Tunisia) has demonstrated that the connectivity of Facebook and Twitter can foment revolution. It showed that while social media may unite those who challenge a system such as Egypt’s where the people’s voice was not heard, they can fragment a society such as United States where every voice is heard. With its proliferation social media has generated a lot of complicated social and legal regulatory issues which are as follows:

2.1.1. Pornography and Obscenity

Sexual depictions which constitute “pornography” or “obscenity” are regulatory concern by the government in both offline and online world. Social media in particular with its fast circulation of obscene and pornographic materials has made regulation more difficult. Various social media websites like YouTube, MySpace and Facebook are loaded with these materials, causing public authorities to work hard to stop this. The difficulty in regulation was well evident when Govt. of India filed a counter before the Supreme Court showing its inability to prevent pornographic and obscene materials on the internet and social media pages. Though there is no specific provision in any statute that directly deals with pornography, it has been brought within the purview of Sec. 292 which deals with obscenity in the Indian Penal Code, 1860 (“IPC”). The Section imposes criminal liability for sale, distribution etc. of obscene material.

41 The Arab Spring, also known as the Arab Revolution is a revolutionary wave of demonstrations and protests occurring in the Arab world that began on 18 December 2010. The importance of the role of social media on the Arab uprisings has been largely debated. Some say that social media was the main instigator of the uprisings; while others claim that it was merely a tool. Either way, the perception of social media has changed; its role in the uprisings has demonstrated to the world its power. Such information allowed the world to stay updated with the protests and facilitated organizing protests. Nine out of ten Egyptians and Tunisians responded to a poll that they used Facebook to organize protests and spread awareness.

42 Kamlesh Vaswani v. Union of India [W.P.(C). No. 177 of 2013 (Supreme Court)], This writ petition was filed before the Supreme Court under Article 32 of the Constitution of India challenging Sections 66, 67, 69, 71, 72, 75, 79, 80 and 85 of the Information Technology Act, 2000 as unconstitutional on the ground that they are inefficient in tackling the rampant availability of pornographic material in India.
Sec. 292 (1) of Indian Penal Code defines obscenity:

“For the purposes of sub-section (2), a book, pamphlet, paper, writing, drawing, painting, representation, figure or any other object, shall be deemed to be obscene if it is lascivious or appeals to the prurient interest or if its effect, or (where it comprises two or more distinct items) the effect of any one of its items, is, if taken as a whole, such as to tend to deprave and corrupt person, who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.”

The definition is very similar to that found in the English Obscene Publications Act, 1959.

Sec. 292 (1) is based on an 1868 English decision (Hicklin Case)\(^{43}\) where the test for obscenity was laid down by Cockburn, C.J as follows:

“….the test of obscenity is this, whether the tendency of the matter charged as obscenity is to deprave and corrupt those whose minds are open to such immoral influences, and into whose hands a publication of this sort may fall............ it is quite certain that it would suggest to the minds of the young of either sex, or even to persons of more advanced years, thoughts of a most impure and libidinous character.”

Under the Indian law though watching pornography is not illegal but sharing or disseminating obscene content has been made punishable under Sec. 67 of the Information Technology Act. The Act provides a penalty of imprisonment up to three years for publishing and transmitting obscene content. There are stricter rules against child pornography.

Supreme Court in Ranjit D. Udeshi vs. State of Maharashtra\(^{44}\) defined obscenity as ‘the quality of being obscene which means offensive to modesty or decency; lewd, filthy and

\(^{43}\) R. v. Hicklin, (1868) LR 3 QB 360
repulsive.’ In this case court drew a difference between obscenity and pornography. It was held that while pornography denotes writings, pictures etc. intended to arouse sexual desire, obscenity may include publications not intended to do so but which have that tendency. While both offend against public decency and morals, pornography is obscenity in a more aggravated form.

The impact of obscenity laws in India can be seen in the unfettered discretion exercised by the Government to ban films, books and other materials on the pretext of immoral or objectionable content in offline world. The approach of the govt. in dealing with obscene contents on internet cannot be equated with offline world. The transnational character of internet provides limited scope and jurisdiction to the govt. authorities in regulation.

In the case of Kamlesh Vaswani vs. Union of India and Others, the petitioner challenged the Sections 66, 67, 69, 71, 72, 75, 79, 80 and 85 of the Information Technology Act 2000 as unconstitutional, as they are inefficient in tackling the rampant availability of pornographic material in India. It was demanded by the petitioners that viewing of pornography be made a non-bailable offence and pornographic content on the internet be blocked. Internet Service Providers Association of India (ISPAI) has submitted that they cannot block such sites and they can only do so only on the direction of the govt. Government submitted that it was struggling to block pornography sites because there were around four crore websites and when they block one, a new one is created. The govt. has further submitted that it has constituted a Cyber Regulation Advisory Committee under Sec. 88 of the IT Act and one of the briefs assigned to that Committee is with regard to availability of Pornography on Internet.

44 AIR 1965 SC 881, Para 7, p. 885

45 In judging as to whether a particular work is obscene, regard must be had to contemporary mores and national standards. While the Supreme Court in India held Lady Chatterley’s lover to be obscene, in England the jury acquitted the publishers finding that the publication did not fall foul of the obscenity test. This was heralded as a turning point in the fight for literary freedom in UK. Perhaps ‘community mores and standards’ played a part in the Indian Supreme Court taking a different view from the jury. The test has become somewhat outdated in the context of internet age which has broken down traditional barriers and made publications from across the globe available with the click of a mouse. See; Ram Jethmalani & D S Chopra, ‘Media Law’ (Second Edition, Vol.-I, Thomson Reuters 2014) 942

46 (2014) 6 SCC 705 (Till the time of writing of this thesis the case was still pending before the Supreme Court)
Although there can be no difference of opinion on this point that a state should control the possession and dissemination of obscene and indecent material in its territory, there is no consensus on what type of content should be considered as obscene or indecent. The sharpest disagreements lie in the field of nudity and depictions of sexuality. Thus for example, in Scandinavia there is general perception that images of naked adults are entirely acceptable, whereas in countries whose law or culture is based on strict orthodox principles, such as Saudi Arabia\textsuperscript{47}, depictions of mere nudity may well be unlawful per se. The states are facing dilemma to how to prevent pornographic materials on the internet which is transnational in character and possessing powers to defy state framed rules and regulations.

The test for determining standard of obscenity also varies widely and intensifies the problems in regulating the obscenity on the internet. In the UK, e.g. the definition of obscenity is based on the potentials effects of the material on its readers or viewers. In Sec. 1(1) of the Obscene Publications Act 1959 obscenity is defined as follows:

\begin{quote}
“an article shall deemed to be obscene if its effect or the effect of any one of its terms is, if taken as a whole, such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.”
\end{quote}

In the case of \textit{DPP vs. A and BC Chewing Gum Ltd}\textsuperscript{48} it was held that the abovementioned definition is not limited to sexually explicit material, and a depiction of violent activity has also been held to tend to deprave or corrupt, and thus to be obscene.

In the US, obscenity is defined in the context of sexual material, and requires the material to appeal to the prurient interest, as defined by reference to the standards of the local community, and to depict sexual conduct defined by the applicable state law.\textsuperscript{49}

\textsuperscript{47} Faiza S Ambah, ‘An Intruder in the Kingdom’ (1995) 21Business Week 40

\textsuperscript{48} \textit{DPP vs. A and BC Chewing Gum Ltd} (1968) 1 QB 159

\textsuperscript{49} \textit{Miller vs. California} (1973) 413 US 15
2.1.2 Hate Speech

The subject of hate speech has gained significance with the increase in communal conflagrations mainly caused communal hate campaigns over the social media websites. In North Eastern Mass Exodus\textsuperscript{50}, Muzaffar Nagar Riots\textsuperscript{51}, investigations revealed that hate contents circulated by social media has sparked communal clashes. Behind nearly half-a-dozen communal clashes in the country, the reason was the content on social media that insulted or humiliated communities.\textsuperscript{52} According to a report\textsuperscript{53} there is a surge of 25 per cent on the growth of "problematic" social networking groups on the Internet. The report was based on "over 10,000 problematic web sites, social networking groups, portals, blogs, chat rooms, videos and hate games on the Internet which promote racial violence, anti-semitism, homophobia, hate music and terrorism."\textsuperscript{54}

Hate speech can be understood as “...antisocial oratory that is intended to encourage persecution against people because of their race, color, religion, ethnic group, or nationality, and has a substantial likelihood of causing . . . harm”.\textsuperscript{55} It has several dimensions e.g. context/content/targets/tone and potential implications of speech.


\textsuperscript{52} Nearly 10 communal clashes have happened throughout Gujarat in 2012. See; Sarfaraz Shaikh & Saeed Khan, ‘Nasty posts on social media are new riot triggers’ (TNN, Oct 6, 2014) <http://timesofindia.indiatimes.com/india/Nasty-posts-on-social-media-are-new-riot-triggers/articleshow/44444221.cms>


\textsuperscript{54} The report also find a mention in K. Jaishankar, ‘Cyber Hate: Antisocial networking in the Internet’ (2008) International Journal of Cyber Criminology, Vol. 2 Issue 2

\textsuperscript{55} Alexander Tsesis, ‘Destructive Messages: How Hate Speech Paves the Way for Harmful Social Movements’ (NYU Press 2002), 211
In a landmark American Judgment, the expression ‘hate speech’ was described by Justice Murphy as:

“fighting words including those which by their very utterance inflict injury or tend to incite an immediate breach of peace to a person or a group of persons. It has been observed that such utterances are no essential part of any exposition of ideas, and are of such slight social value as a step to truth that any benefit that may be derived from them is clearly outweighed by the social interest in order and morality.”\textsuperscript{56}

In India hate Speech does not find place under Article 19 (2) of the Constitution and therefore, does not constitute a specific exception to the freedom of speech and expression under Article 19 (1) (a). However, it is read under other specified exceptions under Article 19 (2) such as ‘sovereignty and integrity of India’, ‘security of the State’, ‘incitement to offence ’, ‘defamation’ etc.

Hate propaganda is controlled by wide range of Indian statutes. Some of the provisions which will apply in hate speech over social media platforms are-

- The Indian Penal Code, 1860 contains provisions which prohibit hate propaganda. Section 153-A penalizes the promotion of class hatred. Section 295-A penalizes insults to religion and to religious beliefs. Section 505 makes it a penal offence to incite any class or community against another.
- The Information Technology Act, 2000 contains several provisions which will apply to mitigate hate campaigns on internet. It includes Sec. 66-A (now unconstitutional), Sec. 69 etc.\textsuperscript{57}

Removing hatred materials on the social media pages is a difficult task. It is easy for one to upload but hard for others to take it down. At the users end Facebook provides an option which enables a user to mark something as obscene/inflammatory/hateful etc. but it then leave it, at the uploader’s choice to remove the hateful content. Even after

\textsuperscript{56} Chaplinsky vs. New Hampshire (1942) 315 U.S. 568

\textsuperscript{57} These provisions have been discussed later in this chapter.
receiving notification of a hateful content most of social media platforms take unreasonably long time to remove it.

At the international level, The International Network against Cyber Hate (INACH), which was started in 2002, is significantly working against cyber hate. INACH Foundation was established under Dutch law and is seated in Amsterdam. The mission of the foundation is to unite and empower organization across the globe to promote respect and responsibility by countering cyber hate and raising awareness about online discrimination. INACH works for the human rights and mutual respect between internet users.

2.1.3 Identity Theft

Identity theft is another problem generated by social media. Since, social media websites generate revenue with targeted advertising, based on personal information; they encourage their users to provide maximum personal/professional information. With limited regulatory oversight by government, industry standards or incentives to educate users on security, privacy and identity protection, they are exposed to identity theft. Phishing on social media websites are being used to trick individuals into providing sensitive information that can be used to steal their identities. The trick may be delivered through the networking website’s messaging system or through an application designed to look like a harmless quiz, survey, or product giveaway.

Many of the users normally post more than enough information about their personal and work lives. The identity thieves could easily compile that information in order to create a fake profile that looks authentic to people who know the user. A fake profile, similar in appearance to original one, may provide ample opportunity to fake profile creator to gain information about the user and his/her friends. And because people often believe that they are sharing the information only with the people they already know, they often publish plenty of details that hackers (fake profile creator) can use to harass.
In India, Information Technology Act provides punishment for identity theft. According to 66-C of the Act-

“Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.”

There is little evidence that users of social networking sites are taking full measures to protect themselves from identity theft. For example, numerous celebrities have claimed their Twitter accounts have been hacked and there are various profiles by their name.\textsuperscript{58,59} According to the Huffington Post, Bulgarian IT consultant Bogomil Shopov claimed in a blog to have purchased personal information on more than 1 million Facebook users, for the frighteningly low price of $5.00. The data reportedly includes users' full names, email addresses and links to their Facebook pages.\textsuperscript{60}

\section*{2.1.4 Intellectual Property Issues}

\begin{itemize}
  \item Trademark infringement and dilution
  \item Copyright infringement
  \item Trade secret disclosure
\end{itemize}

\textsuperscript{58} Alex Myers, ‘After a Twitter hack, ‘biebermyballs’ becomes a popular hashtag’ (daily caller, 28 March, 2012) \texttt{<http://dailycaller.com/2012/03/28/after-a-twitter-hack-biebermyballs-becomes-a-popular-hashtag/>} accessed on 02 May 2013

\textsuperscript{59} Facebook has deleted the original profile of Dr. Subramanyam Swamy, when he demanded for removal of fake profiles in his name. See; FP Staff, ‘Oops! Facebook accidentally deletes Subramanian Swamy's real account, parody page lives on’ (First Post, 19 Dec 2014) \texttt{<http://www.firstpost.com/living/oops-facebook-accidentally-deletes-subramanian-swamys-real-account-parody-page-lives-on-1857147.html> } accessed on 20 Dec. 2014

\textsuperscript{60} Ryan Grenoble, ‘Bogomil Shopov, Bulgarian Tech Consultant: 1 Million Users' Private Facebook Data Available Online For $5’ (The Huffington Post, 27 Oct. 2012) \texttt{<http://www.huffingtonpost.com/2012/10/26/bogomil-shopov-facebook-data_n_2024133.html> } accessed on 02 May 2013
A. Trade Mark Infringement and Dilution

On social media platforms, users discuss, create content and interact with brands more than ever before. Most often it results into harmful information about goods/services which injure a brand mark’s strength/reputation/goodwill. A quick search for any major brand name on Facebook will often reveal hundreds of results, which typically include some official results (often labelled ‘official’) and many unofficial results. The prevalence of various contents/pages in the same name often attempts to tarnish the image of famous brands. For example, news of fried rat served instead of chicken in KFC (a famous non veg food chain) has made a top trend in Facebook after the California based man complained about this. But later it was found to be a deliberate attempt to tarnish the KFC image.

There are very little measures to prevent an individual or entity from adopting a user name or sub-domain name that incorporates a third party's registered trade mark. Taking remedial action can often be problematic for the trade mark owner, both from the sheer scale of the problem, to considering issues of adverse publicity that may make a bad situation worse.

Further, Improper dilution of famous marks is another area of concern regarding trade mark infringement. It can be done in two ways:

Blurring – occurs in social media when a user uses a famous mark in connection with other goods/services. For example

- User may use its postings to advertise luxurious BENTLEY clothing, jewellery

---


• Owner of the famous BENTLEY mark for automobiles does not want to permit usage of its famous mark on such goods

Tarnishment – occurs in social media when a user associates a famous mark with substandard goods/services which results in damage to famous mark’s reputation and injury to famous mark’s goodwill

Apart from it, improper comparative advertising can result into a trade mark misuse on social media platforms. For example

- False/misleading advertising
- Competitors may use each others’ trademarks to compare goods/services to divert sales

In addition, there is a lot of uncertainty over the use of trade marks in social media and there is uncertainty as to whether current trademark laws and enforcement techniques adequately address the trademark issues presented by social networking sites. Both Twitter and Facebook have trade mark policies but they are not well drafted when it comes to dealing with trade mark infringement issues and the practical enforcement of those policies.

Twitter's trade mark policy provides:

"Using a company or business name, logo or other trademark-protected materials in a manner that may mislead or confuse others or be used for financial gain may be considered to be trademark infringement. Accounts with clear INTENT to mislead others will be immediately suspended; even if there is no trademark infringement, attempts to mislead others are tantamount to business impersonation".64

Twitter has also adopted a specific impersonation policy, stating that:

---

"non-parody impersonation is a violation of the Twitter Rules...An account may be guilty of impersonation if it confuses or misleads others – accounts with the clear INTENT to confuse or mislead will be permanently suspended."65

Facebook's IP infringement policy provides:

"Facebook is committed to protecting the intellectual property of third parties. On this page, rights owners will find information regarding how to report copyright and other intellectual property infringements by users posting content on our website".

The practical operation of Twitter's policy was put to the test in a US case.66 Natural gas distributor Oneok Inc. sued Twitter, Inc. in federal court in Oklahoma for direct and contributory trademark infringement. The petitioner in this case claimed that Twitter has wrongfully allowed an unauthorized third party to adopt its username "ONEOK", which was not just its corporate name but also a registered trade mark. The unauthorized user posted tweets about ONEOK which ONEOK Inc said were misleading as they had the hallmark of appearing like an official statement from ONEOK Inc when they were not. ONEOK Inc sought to resolve the issues directly with Twitter and asked Twitter to invoke its trademark policy and terminate or transfer the offending account to them. ONEOK Inc's direct correspondence with Twitter was unsuccessful but after it issued proceedings for trade mark infringement, the account was then transferred to ONEOK Inc.

65 Twitter, ‘Impersonation Policy’ (Trademark) <https://support.twitter.com/articles/18366-impersonation-policy> accessed on 05 May 2014

B. Copyright Infringement

The Copyright Act, 1957 (Act No. 14 of 1957) governs the laws & applicable rules related to the subject of copyrights in India. The Copyright Act is compliant with most international conventions and treaties in the field of copyrights. India is a member of the Berne Convention of 1886 (as modified at Paris in 1971), the Universal Copyright Convention of 1951 and the Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS) Agreement of 1995. Though India is not a member of the Rome Convention of 1961, WIPO Copyrights Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT), the Copyright Act is compliant with it.

Copyright is a right given by the law to the creators of literary, dramatic, musical and artistic works and producers of cinematograph films and sound recordings. In fact, copyright is a bundle of rights which includes rights of reproduction, communication to the public, adaptation and translation of the work. The law permits that; there can be slight variations in the composition of the rights, depending on the work.

The growth of internet and the increasing popularity of social media have resulted in an increase in copyright infringement. The multimedia world of the social web is littered with copyright materials, which may or may not be reproduced with the consent of the right owners. Photographs posted to Facebook and Flick, films and music posted to YouTube and materials posted on a blog or on wikis may not always be a matter of copyright protection. Users infringing the rights of copyright owners are liable to be sued for infringement. 67 But there are two challenges in this respect-

- Determining ownership of User Generated Content
- Determining liability

67 The British Phonographic Industry, which represents the records companies and other major stakeholders in the UK music industry, started (successfully) taking legal action against members of file sharing communities for copyright infringement in 2005. See; Peter Wainman, ‘BPI sues file sharers’ (Naked Law, 02 Aug, 2005) <http://nakedlaw.typepad.com/naked_law/2005/08/the_bpi_has_iss.html> accessed on 26 Oct. 2013
Users often believe that they own the personal data that they feed about themselves on social media.\textsuperscript{68} Fact is that no one owns facts. Factual information is largely excluded from intellectual property law protection: copyright law protects only creative expression, not factual information. Further, personal information about the user and others post on social media is not a secret therefore it cannot be subjected to trade secret law protection. When social media companies aggregate information about usage and user preferences, the social media companies can claim trade secret ownership rights in such aggregate information, but they own such trade secrets and user do not. Also, databases with content and personal information can be protected under European database laws and U.S. state laws on appropriation, but again, as property of the social media companies and not as user’s personal property. So, if anyone owns personal data about the users, it is the social media companies, not the user.\textsuperscript{69} It is also difficult to determine the liability for social media contents. Sometimes user or internet service provider may be held liable for the contents individually but sometimes both of them can be equally liable the contents.

ISPs also run the risk of being exposed to claims of copyright infringement. Most famously, Napster was found liable in the U.S.A. for contributing to the infringement of copyright by its users, who were sharing music files over a peer to peer network. In this case the musician has required YouTube to remove infringing copies of his music and has threatened to sue You Tube for contributory infringement.\textsuperscript{70}

C. Trade Secret Disclosure

Social media and trade-secret protection represents a new frontier – one with relatively little case law, but with substantial implications. A customer list is the most notable area in which social media can affect a company’s protection of its confidential information.

\textsuperscript{68} Paula Samuelson, ‘Privacy as Intellectual Property?’ (2000) 52 Stan. L. Rev. 1125, 1130

\textsuperscript{69} Lother Determann, ‘Social Media Privacy: A Dozen Myths and Facts’ (2012) 7 Stan. Tech. L. Rev.

Employers often encourage their sales personnel to use LinkedIn or other social media platforms to establish and strengthen relationships with actual and potential customers. But sometimes this relationship raises question regarding ownership of that social-media account when salespeople leave and go to a rival company? The sales personnel leave the company with a de facto customer list. It is likely that the names and contact information of some or all of a salesperson’s key client relationships will reside on that social-media account.71

*Sasqua Group, Inc. vs. Courtney*72

In this case Executive search firm sued former employee for misappropriation of trade secrets. The employee was charged for misappropriating the client list of the company. The court observed that

“A customer list developed by a business through substantial effort and kept in confidence may be treated as a trade secret provided the information it contains is not otherwise readily ascertainable.”

But because the information could be pieced together from LinkedIn and other Internet sites, the court held it did not constitute a trade secret.

*PhoneDog LLC vs. Kravitz*73

In this case the petitioner claimed that its former employee stole trade secrets by keeping and using a Twitter account opened while employee worked for PhoneDog. Ex-employee has changed name from @PhoneDog_Noah to @noahkravitz but continued to use the following built up under prior name. Accepting the arguments of the company as substantial the court has allowed the case to go further.

---

73 case no. 3:11-cv-03474
Another associated legal issue is of the disputes regarding the ownership of social networking accounts after an employee who maintains the account leaves the company? Three lawsuits highlight the challenges an employer may face in seeking to gain control of work-related social media accounts maintained by current or former employees.

_Eagle vs. Edcomm_74

In the present case LinkedIn password of former CEO of a company has been changed by the company when she left the company. Ex employee has filed a suit before the court. The Court has made two orders. First order says that “LinkedIn connections were not a trade secret because they are either generally known in the wider business community or capable of being easily derived from public information.” Secondly, “plaintiffs apprehension of ‘reputation’ ‘goodwill’ and ‘business opportunity’ are insufficient to satisfy the ‘loss’ element of company.”

_Blands vs. Roberts_75

Former employees of an office, who were fired, sued the office claiming that they were fired for having supported an opposing candidate in a local election. Both the plaintiffs had “liked” the opposing candidate’s Facebook page, which they claimed was an act of constitutionally protected speech. A federal district court in Virginia, however, ruled that a Facebook “like” “. . . is insufficient speech to merit constitutional protection”; according to the court, “liking” involves no actual statement, and constitutionally protected speech could not be inferred from “one click of a button.”

This case explored the increasingly important intersection of free speech and social media with the court finding that a “like” was insufficient to warrant constitutional protection.

_New York vs. Harris_76

In early 2012, the New York City District Attorney’s Office subpoenaed Twitter to produce information and tweets related to the account of defendant. Twitter first sought

---

74 Case 2:11-cv-04303-RB
75 No. 12-1671 (4:11-cv-00045-RAJ-TEM)
76 2012 NY Slip Op 22109 (36 Misc 3d 613)
to quash the subpoena, but the court denied the motion, finding that it had no proprietary interest in the tweets and therefore did not have standing to quash the subpoena. Twitter then filed a motion to quash, but the court also denied its motion, finding that present defendant had no reasonable expectation of privacy in his tweets, and that, for the majority of the information sought, no search warrant was required.

This case set an important precedent for production of information related to social media accounts in criminal suits. According to the court’s decision, in certain circumstances, a criminal defendant has no ability to challenge a subpoena which requires a particular social media account information and details of its contents.

These legal complexities have taken many forms. There are three notable examples in United States in which the first one is Jake Baker incident\(^77\), second is the controversial distribution of the DeCSS software code\(^78\), which decodes the content-scrambling system used for DVD licensing enforcement, and third is Gutnick vs. Dow Jones\(^79\), in which libel laws were considered in the context of online publishing. The last example was particularly significant because it epitomized the complexities inherent to applying one country's laws (nation-specific by definition) to the internet (international by nature).\(^80\)

### 2.1.5 Defamation

A major issue in the social media context is defamation. Generally speaking a defamatory statement is a false and disparaging statement about another that causes injury to

\(^77\) It concerns the alleged obscene internet postings by a student at the University of Michigan to express his fantasies regarding a female student of his acquaintance. His actions and the response by the university authorities and ultimately by the FBI raise interesting questions about the status of electronic postings in the whole domain of freedom of expression and even more on the control required by those who operate newsgroups.


\(^79\) (2002) HCA 56

reputation of the person to whom it refers and exposes him to hatred, ridicule, or contempt, or which causes him to be shunned or avoided. The Indian Penal Code makes it a punishable offence.\textsuperscript{81} The section requires three essentials:

- Making or publishing any imputation concerning any person
- Such imputation must have been made by- (a) words, either spoken or intended to be read; or (b) signs; or (c) visible representations.
- Such imputation was made with the intention of harming or with knowledge or reason to believe that it will harm the reputation of the person concerning to whom it is made.

The unmediated character of social media increases its potential for defamatory use. When we consider the essential elements of defamation in the context of defamation on social media pages, the following questions arise:

- When does a publication take place?
- How does a publication take place?
- Where does the publication take place?
- Who is liable for the publication?

Publication-

For the offence of defamation publication of defamatory matter is essential. In other words the defamatory matter must be communicated to some person other than the person to whom it concerns. Publication of the defamatory statement takes place when the content of a statement are seen or heard by the reader or the hearer. An electronic publication could take place through the email, online bulletin board messages, chat room messages, music downloads, audio files, streaming videos, digital photographs and so on. Section 499 of the Indian Penal Code, 1860 expressly provides that defamation could take place not only by words but also by signs or visible representations. This would

\textsuperscript{81} Section 499 of Indian Penal Code defines defamation and Section 500 provides punishment for defamation.
mean that even dissemination of defamatory material through the SMS, MMS, Photographs and Videos or mobile phones would constitute an actionable claim.\textsuperscript{82}

Place of publication and jurisdiction-

An online defamatory statement can be published anywhere in the world where internet is available. This raises jurisdictional issues since technically; a suit would be maintainable in any jurisdiction in the world where the statement has been accessed. Therefore, a defendant could be dragged to any jurisdiction where the statement is accessed notwithstanding where he had posted the information. The place of publication, that is the place where the material is read, heard or seen is the basis of the cause of action for defamation.

Liability determination-

Fixing the liability for defamatory material between ISPs & information publisher is another important aspect of online defamation. At first, the information publisher would he held liable but the role of ISPs in promoting defamatory material shall also be considered. Failure of ISPs in removing the defamatory material on the demand of victim would be a ground to establish the liability of ISPs. The liabilities of the ISPs have been discussed later in this chapter.

\textbf{2.1.6 Privacy Violation by Social Media}

While the idea of ‘privacy’ is venerable, modern obsessions with privacy are largely rooted in the twentieth century.\textsuperscript{83} The unprecedented level of information dissemination on social media websites invariably has implications on user’s personal privacy. A vast majority of social networking sites set a particular privacy setting as default so that anyone can see a person’s information unless privacy settings are actively changed. As a

\textsuperscript{82} Madhavi Goradian Divan, ‘\textit{Facets of Media Law}’ (Reprint, EBC, 2010) 109

\textsuperscript{83} Andrew T. Kenyon & Megan Richardson (eds.), ‘\textit{New Dimensions in Privacy Law}’ (Reprint, Cambridge University Press 2007) 1
result, considerable number of the users inadvertently allows public access to parts of their personally identifying information merely by failing to actively change their privacy settings.\(^{84}\) This criticism is vindicated by a study that points out that 41 percent child and 44 percent adult Facebook users have open privacy settings, mostly arising out of a failure to change the default settings.\(^{85}\) However the problem of privacy violation persists for technology aware users also who have actively changed their default settings because a lot of their information may be available on their friend’s social media page. For instance, a user may be tagged in a photograph or comment posted by a friend and is unable to exercise any control over how that data is presented and what privacy settings are applied by the friend.

Websites and advertising companies are able to track user as they travel on the internet to assess their personal preferences, habits and life styles. It is possible because every time a user log on to the internet he leaves behind an electronic trail. This information is used for direct marketing campaigns that target the individual customer. For example if a user spares little time at some online shopping store like myntra.com, then he will automatically start getting suggestions of new offers from myntra.com at his social media pages. This situation leads only to a logical conclusion that somewhere social networking sites are sharing personal information of the user for revenue purposes.

Another area of privacy violation in social networks is the permanent availability of user’s information to others. For example Facebook does not delete complete information of the user even if he permanently deletes his account. Facebook’s data use policy says:

> “When you delete your account, it is permanently deleted from Facebook. It typically takes about one month to delete an account, but some information may remain in backup copies and logs for up to 90 days. You should only delete your account if you are sure you never want to reactivate it. You can delete your account.”


Certain information is needed to provide you with services, so we only delete this information after you delete your account. Some of the things you do on Facebook aren’t stored in your account, like posting to a group or sending someone a message (where your friend may still have a message you sent, even after you delete your account). That information remains after you delete your account.”

Any picture captured during video chat in Gmail is automatically saved in Google plus which is Google’s social media platform. The user is never informed about the automatic save function of Gmail to Google plus. Thankfully the stored album is set ‘private’ by default. The permanent availability and saving without the knowledge/consent of the users is a gross violation of user’s right to know. Ironically, the policy of Google plus says that even if the user deletes his account the pictures will not be deleted. Further, it takes 60 days for Google plus to permanently delete any material from the trash.

Another major concern is the complexity and incomprehensible nature of the privacy policies and terms of use of most social networking sites. Among other victims of this problem was the winner of an American beauty pageant– Miss New Jersey, 2007. Under the impression that her album was restricted to her Facebook friends only, she posted some racy photographs on the site. To her utter surprise, she was soon blackmailed by another Facebook user who gained access to the album. While the fault in this case may be attributed to the victim, it is not difficult to imagine that a larger number of users are left in the dark owing to the complexities of the websites complex privacy controls. Facebook itself in a blog post admitted that most new users of Facebook had their privacy setting set at “public” which have resulted in some users accidentally sharing information

86 Facebook, ‘Data Policy’ (Facebook, 30 January 2015) <https://www.facebook.com/about/privacy/your-info> accessed on 10 March 2014


with too many people. 89 In the same post, Facebook revealed its plan that now privacy setting for news users would be set ‘friends only’ by default.

(i) Privacy and the right to free speech

The right to freedom of speech and expression and the right to privacy are two sides of the same coin. One person’s right to know and be informed may violate another’s right to be left alone. Just as the freedom of speech and expression is vital for the dissemination of information on matters of public interest, it is equally important to safeguard the private life of an individual to the extent that it is unrelated to public duties or matters of public interest. The law of privacy endeavours to balance these competing freedoms.90

(ii) Privacy and the Law

Article 12 of Universal Declaration of Human Rights and Article 17 of International Covenant on Civil and Political Rights, 1966 reads:

“No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”

Article 8 of the European Convention on Human Rights, 1950 reads:

“Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country,


90 Madhavi Goradian Divan, ‘Facets of Media Law’ (Reprint, EBC 2010) 113
for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”

There are also a few statutory provisions contained in the Code of Criminal Procedure, 1973 [Sec. 327 (1)], the Indecent Representation of Women (Prohibition) Act, 1980 (Section 3 & 4), The Medical Termination of Pregnancy Act, 1971 (Section 7 (1) (c)), The Hindu Marriage Act, 1955 (Section 22), The Special Marriages Act, 1954 (Section 33), The Children Act, 1960 (Section 36), and the Juvenile Justice Act, 1986 (Section 36) which seek to protect women and children from unwarranted publicity.

In India Article 19 (2) does not expressly enumerate ‘privacy’ under ‘reasonable restrictions’ but this lacuna has not prevented the courts from carving out a constitutional right to privacy by a creative interpretation of the right to life under Article 21. Supreme Court of India has developed the law on the privacy in a series of cases. Surveillance power of state police was first considered in Kharak Singh vs. State of U.P. The Court has struck down a regulation which authorized domiciliary visits as being unconstitutional. After this case police power of surveillance has been settled by Supreme Court in Govind vs. State of M.P. & Malak Singh vs. State of P & H. However, till date Supreme Court has not discussed privacy issues in cyber world.

2.1.7 Cyber Bullying and Harassment

According to the US National Crime Prevention Council, cyber bullying happens when the internet, cell phones or other devices are used in cruelty to others by sending or posting text or images intended solely to hurt or embarrass another person.

---

91 AIR 1963 SC 1295
92 (1975) 2 SCC 148
93 (1981) 1 SCC 420
Cyber bullying allows the offender to conceal his identity behind a computer. This anonymity makes it easier for the offender to act against victim without having to see the victim’s physical response. The distancing effects provided by technological devices have its impact on offenders and it often leads them to say and do crueler things compared to traditional face-to-face bullying situation.

Online publication of personal information on social media pages is prone to bullying because it can lead to disclosure of those information’s also which are kept private in real lives. This vulnerability puts many users in a position as either the victim or active offender partaking in cyber bullying actions. Another aspect of social media that can be misleading and hazardous is the ability to create fake profiles. Fake profiles provide an opportunity to say anything to another individual without the worry of any repercussions.

Anonymous blogging has also fostered cyber bullying and fuelled ethical debate. In US, websites, such as College ACB and Juicy Campus, both have faced tightened regulations due to their verbally abusive nature. The forum in these sites included various harsh topics for debate/discussion. Equal feature is provided by various other social media websites most often results into abusive comments.94

2.1.8 Social Media & Freedom of Speech and Expression

Through social media, the monolith of speech has infiltrated all forms of space. In a democratic country like India where Right to Freedom of Speech and Expression has been expressly guaranteed as fundamental right under the constitution, it is terribly clear that this right cannot be taken away except under the situations mentioned in Article 19(2).95 Time and again this fundamental right has taken a course which may well be


95 Article 19 (1) (a) of the Constitution of India also confers on the citizens of India the right “to freedom of speech and expression”. The freedom of speech and expression means the right to express one’s convictions and opinions freely by word of mouth, writing, printing, pictures or any other mode. It also includes the right to propagate or publish the views of other people. Article 19 (1) All citizens shall have the right—
(a) to freedom of speech and expression;
counted as a threat to laws and policies initiated by the govt. and have resulted in a debate whether these rights can be curtailed. Advancement of technologies particularly in social media arena has added a fuel to the fire because it has provided common masses to have their say on public platform.

Freedom of expression is the most cherished right in our Constitution as protected under Art. 19 (1) (a) which is also restricted by what is set out in Art. 19 (2), empowering the state to make appropriate law in that regard. However, even when State does not interfere, the Freedom of Expression is not as free as it should be. As suggested by Dr. Justice Rajendra Babu market forces and controls by society or public at large restrict such rights. For example banning of Salman Rushdie book ‘satanic verses’, banning of Mani Ratnam’s film ‘Bombay’ in Bombay and when film director Deepa Mehta could not show several of her movies including ‘fire’ and ‘water’ in India. These incidences show the curtailment of freedom of expression in India without any legal backing. Such incidences are clearly in the violation of Supreme Court judgment in *L.I.C vs. Manubhai D. Shah* & *Ministry of Information and Broadcasting, Government of India vs. Cricket Association of Bengal*. These above discussed judgments say that the right to freedom of speech and expression would include the freedom of a citizen as a viewer/listener/reader to receive and to communicate or disseminate information and ideas without interference. It is the constitutional obligation of the state to ensure

(b) to assemble peaceably and without arms;
(c) to form associations or unions;
(d) to move freely throughout the territory of India;
(e) to reside and settle in any part of the territory of India; [and]
(f) to practise any profession, or to carry on any occupation, trade or business.
(2) Nothing in sub-clause (a) of clause (1) shall affect the operation of any existing law, or prevent the State from making any law, in so far as such law imposes reasonable restrictions on the exercise of the right conferred by the said sub-clause in the 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.

---

96 Rajendra Babu, 'Transcripts of Lecture delivered at G.N. Sabahit Memorial 2004’ 1 Karnataka State Law University Journal 1

97 1992(3)SCC 637

98 1995 (2) SCC 161
conditions in which these rights can be meaningfully and effectively enjoyed by all citizens and prevent its monopoly or dominance by a few.

It is very interesting to note that the Supreme Court in *Tata Press Ltd. Vs. Mahanagar Telephone Nigam Ltd* held that, commercial speech is a part of freedom of speech and expression guaranteed under Article 19(1)(a). Therefore, commercial advertisement is a form of commercial speech and is protected under Article 19(1)(a) subject to Article 19(2). A very interesting situation arises when we extend this ruling to advertisements over social media websites.

- Does commercial speech as fundamental right of one may subjugate other’s fundamental right to freedom of what to see and what not?
- How can one claim the freedom of speech and expression against the social media web when it is enforceable only against state? [In India, internet service providers are both state-owned (BSNL and MTNL), and privately-owned (Airtel, Spectranet, Reliance, Sify etc). Given that most of the ISPs are privately owned, how does the Constitution even come into the picture? Our fundamental rights are enforceable vertically, that is, between individuals and the State, and not horizontally – that is, between two individuals, or two private parties.

In the first situation, it appears that the actual problem lies with ‘terms and conditions’ stipulated by social networking sites and due regard should be paid to contractual clause which mention about the advertisements. Most of social networks offer their services free of cost they make money with advertisements. In the process they allow bulk of advertisements to be shown on their pages without any involvement of user. People who use social networks store various information about themselves including, but not limited to, their age, gender, interests, and location. This stored information allows advertisers to create specific target groups and individualize their advertisements. While it is clear that social media websites feature advertisement according to the interest of users it also raises question about sharing of user’s personal information to the advertising companies.

---

99 1995 AIR 2438
Coming to the second situation it would be pertinent to analyze Article 12 of Indian Constitution which says-

“In this part, unless the context otherwise requires, the State includes the Government and Parliament of India and the Government and the Legislature of each of the States and all local or other authorities within the territory of India or under the control of the Government of India.”

The Supreme Court has struggled with the issue of defining “other authorities” for the purposes of Part III of the Constitution, with the pendulum swinging wildly at times. In the case of Pradeep Kumar Biswas v. Indian Institute of Chemical Biology\(^{100}\), a 2002 judgment by a Constitution bench, the Court settled upon the following definition:

“The question in each case would be whether in the light of the cumulative facts as established, the body is financially, functionally and administratively dominated by or under the control of the Government. Such control must be particular to the body in question and must be pervasive. If this is found then the body is a State within Article 12. On the other hand, when the control is merely regulatory whether under statute or otherwise, it would not serve to make the body a State.”

There is no way to argue that ISPs are under the pervasive financial, functional and administrative domination or control of the State. The test laid down by the court in this case seems to be radically under-inclusive. For example if the government decides to privatize the nation’s water supply to private company X. Company X is the sole distributor of water in the country. On gaining control, it decides to cut off the water supply to all households populated by members of a certain religion. There seems something deeply wrong in the argument that there is no remedy under discrimination

\(^{100}\) (2002) 5 SCC 111
law against the conduct of the company. In light of Pradeep Kumar Biswas, it is
obviously difficult to hold the direct application of the Constitution to private entities.¹⁰¹

2.2 ADDRESSING THE PROBLEMS

2.2.1. GOVERNING LAWS

Although there is no specific legislation in India which deals with social media, but there
are variety of laws that will be applicable. Each problem as discussed above is addressed
with different set of laws. These laws were given dominant support by IT Act to counter
the new challenges posed by information technology.

A. The Information Technology Act, 2000¹⁰²

➢ Section 66A of the IT Act has been widely for social media offences. However this
   provision has been held unconstitutional by the Supreme Court.¹⁰³
➢ Section 66C of the IT Act provides punishment for identity theft.¹⁰⁴
➢ Section 66D: Punishment for cheating by personation by using computer resource¹⁰⁵

¹⁰¹ Gautam Bhatia, ‘Net Neutrality, Free Speech and the Indian Constitution – I’ (CIS-India, April 14,
   part-1> accessed on 27 April 2014

¹⁰² India passed the Information Technology Act 2000 in May 2000 in pursuance of the United Nations
   General Assembly Resolution A/RES/51/162 of 30th January 1997. This Resolution adopted the Model
   Information Technology Act, 2000 came into force on 17th October 2000 and it has been substantially
   amended through the Information Technology (Amendment) Act, 2008.

¹⁰³ Shreya Singhal vs. Union of India, (2015) 5 SCC 1; See, Chapter 6 for detailed discussion of the case

¹⁰⁴ It says that “Whoever, fraudulently or dishonestly make use of the electronic signature, password or any
   other unique identification feature of any other person, shall be punished with imprisonment of either
description for a term which may extend to three years and shall also be liable to fine which may extend to
rupees one lakh.”

¹⁰⁵ “Whoever, by means of any communication device or computer resource cheats by personation, shall be
   punished with imprisonment of either description for a term which may extend to three years and shall also
   be liable to fine which may extend to one lakh rupees.”
➤ Section 66E is of utmost importance. Privacy violation of a person without his consent has been made punishable by virtue of this provision.  

➤ Cyber terrorism which has been made more proliferate by social media has also been made punishable by Section 66-F of the Act.

➤ Obscenity in electronic form which is very much prevalent on social media website will come under Section 67 of the Act, which makes it punishable to transmit or publish any obscene material.

➤ Section 67A provides punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form.

106 Section 66E: 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 ..................... private place.”

107 Section 66F: Punishment for cyber terrorism

“(1) Whoever,-

(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –

(i) denying or cause the denial of access to any person authorised to access computer resource; or

(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or

(iii) Introducing or causing to introduce any Computer Contaminant.

and by means .................................. commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.”

108 Section 67: Punishment for publishing or transmitting obscene material in electronic form-

“Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.”

109 According to Section:

“Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with
➢ Section 67B provides punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form.

➢ Section 69 of the Act grants power to the Central or a State Government to issue directions for interception or monitoring or decryption of any information through any computer resource in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States, public order, for preventing incitement to commission of any cognizable offence, for investigation of any offence.

➢ Section 69A grants power to the Central Government to issue directions to block public access of any information through any computer resource on similar grounds.

➢ Section 79 provides for liability of intermediary. An intermediary shall not be liable for any third party information, data or communication link made available or hosted by him.

imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

110 “Whoever,-

(a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct or

(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner or

(c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource or

(d) facilitates abusing children online or

(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children,

shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.”

111 Under section 79 of the IT Act, Intermediaries has been exempted from liability in certain case.

Sec. 79 – “Exemption from liability of intermediary in certain cases
Section 70B provides for an agency of the Government to be appointed by the Central Government called the Indian Computer Emergency Response Team, which shall serve as the national agency for performing functions relating to cyber security.

The Central Government has also enacted rules to give effect to various provisions of this Act which are as follows:

The Information Technology (Procedure and Safeguards of Interception, Monitoring and Decryption of Information) Rules, 2009

These rules have been framed by the Central Government in exercise of its powers under Section 87(2) (y) of the Act having regard to the procedure and safeguards for monitoring and collecting traffic data or information under Section 69B (3). Rule 4 provides for an agency of the Government authorized by the competent authority to carry out the functions. Rule 13 requires the intermediary to provide all facilities, cooperation and assistance for interception or monitoring or decryption of information.

(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link hosted by him. (corrected vide ITAA 2008)

(2) The provisions of sub-section (1) shall apply if-
(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored; or
(b) the intermediary does not-
   (i) initiate the transmission,
   (ii) select the receiver of the transmission, and
   (iii) select or modify the information contained in the transmission
(c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf (Inserted Vide ITAA 2008)

(3) The provisions of sub-section (1) shall not apply if-
(a) the intermediary has conspired or abetted or aided or induced whether by threats or promise or otherwise in the commission of the unlawful act (ITAA 2008)
(b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

Explanation:- For the purpose of this section, the expression ‘third party information’ means any information dealt with by an intermediary in his capacity as an intermediary.”
The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009

These rules are made by the Central Government in exercise of its powers under Section 87(2) (z) with regard to the procedure and safeguards for blocking for access by the public under Section 69A (2).

Rules 3 to 8 of these rules provide for the method of sending request for blocking to the Nodal officer of concerned organization who shall examine it and forward it to the Designated Officer of the Central Government who shall further examine it along with a Committee and then, their recommendation shall be sent to the Secretary, Department of IT for his approval. After receiving such recommendation the Designated Officer shall direct blocking. However, In order to meet the emergency situations rule 9 grants power to the Designated Officer to take a decision regarding blocking.

Rule 13 provides that every intermediary shall designate a person to receive and handle directions for blocking of information. The concerned person shall acknowledge receipt of the directions to the Designated Officer within two hours through acknowledgment letter or fax or e-mail. Rule 10 provides that the Designated Officer, on receipt of a court order directing blocking of any information, shall submit it to the Secretary, Department of Information and Technology and initiate action immediately.

The Information Technology (Intermediaries Guidelines) Rules, 2011

The Intermediaries Guidelines Rules, 2011, enacted under Section 79 of the Act makes it clear that intermediaries must follow in order to be exempt from liability in connection with services rendered by them. The rules impose the responsibility of blocking certain kinds of content upon the intermediaries.  

Rule 3 makes it mandatory for the intermediaries to inform the users to not to host, display, upload, modify, publish, transmit, update or share any information which is

objectionable under Rule 3(2). The information to not to publish obscene content should be mentioned on the websites. If a violation under Rule 3(2) is noticed by or is brought to actual knowledge of any intermediary by an affected person in writing or through e-mail, Rule 3(4) requires the intermediary to remove the objectionable content within 36 hours.

B. Indian Penal Code, 1860

- Section 153-A penalizes the promotion of class hatred.\textsuperscript{113}
- Section 295-A penalizes insults to religion and to religious beliefs.\textsuperscript{114}

\textsuperscript{113} “Promoting enmity between different groups on grounds of religion, race, place of birth, residence, language, etc., and doing acts prejudicial to maintenance of harmony

(1) Whoever-

(a) by words, either spoken or written, or by signs or by visible representations or otherwise, promotes or attempts to promote, on grounds of religion, race, place of birth, residence, language, caste or community or any other ground whatsoever, disharmony or feelings of enmity, hatred or ill-will between different religious, racial, language or regional groups or castes or communities, or

(b) commits any act which is prejudicial to the maintenance of harmony between different religious, racial, language or regional groups or castes or communities, and which disturbs or is likely to disturb the public tranquility, [or]

[(c) organizes any exercise, movement, drill or other similar activity intending that the participants in such activity shall use or be trained to use criminal force or violence or knowing it to be likely that the participants in such activity will use or be trained to use criminal force or violence, or participates in such activity intending to use or be trained to use criminal force or violence or knowing it to be likely that the participants in such activity will use or be trained to use criminal force or violence, against any religious, racial, language or regional group or caste or community and such activity for any reason whatsoever causes or is likely to cause fear or alarm or a feeling of insecurity amongst members of such religious, racial, language or regional group or caste or community,]

shall be punished with imprisonment which may extend to three years, or with fine, or with both.”

\textsuperscript{114} Sec. 295A- “Deliberate and malicious acts, intended to outrage religious feelings of any class by insulting its religion or religious beliefs

Whoever, with deliberate and malicious intention of outraging the religious feelings of any class of [citizens of India, by words, either spoken or written, or by signs or by visible representations or otherwise], insults or attempts to insult the religion or the religious beliefs of that class, shall be punished with imprisonment of either description for a term which may extend to 148[three years], or with fine, or with both.”
Section 505 makes it a penal offence to incite any class or community against another.115
Section 499 for defamation.116
Section 292 applies for obscenity.117

C. Criminal Procedure Code, 1973
Section 166 A is related to Letter of request to competent authority for investigation in a country or place outside India.118

---

115 Sec. 505.- “Statements conducting to public mischief-

(1) Whoever makes, publishes or circulates any statement, rumour or report,-

(a) with intent to cause, or which is likely to cause, any officer, soldier, sailor or airman in the Army, Navy or Air Force of India to mutiny or otherwise disregard or fail in his duty as such; or

(b) with intent to cause, or which is likely to cause, fear or alarm to the public, or to any section of the public whereby any person may be induced to commit an offence against the State or against the public tranquility; or

(c) with intent to incite, or which is likely to incite, any class or community of persons to commit any offence against any other class or community;

shall be punished with imprisonment which may extend to three years, or with fine, or with both.

(2) Statements creating or promoting enmity, hatred or ill-will between classes Whoever makes, publishes or circulates any statement or report containing rumour or alarming news with intent to create or promote, or which is likely to create or promote, on grounds of religion, race, place of birth, residence, language, caste or community or any other ground whatsoever, feelings of enmity, hatred or ill-will between different religious, racial, language or regional groups or castes or communities, shall be punished with imprisonment which may extend to three years, or with fine, or with both.

Exception- It does not amount to an offence, within the meaning, of this section when the person making, publishing or circulating any such statement, rumour or report, has reasonable grounds for believing that such statement, rumour or report is true and makes, publishes or circulates it in good faith and without any such intent as aforesaid.”

116 Sec. 499- Defamation

“Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter expected, to defame that person.........................

..............Public good.”

117 Sec. 292- “Sale, etc., of obscene books, etc. _

(1) For the purposes of subsection (2), a book, pamphlet, paper, writing, drawing, painting, representation, figure or any other object,.................................religious purpose.”

118 See; Chapter 3 for detailed discussion
Section 4 is related to trial of offences under the Indian Penal Code and other laws.\textsuperscript{119}

Section 188 is related to offence committed outside India.\textsuperscript{120}

\textbf{2.2.2. GOVERNING AUTHORITIES}

The nature, function and organizational structure of the regulatory authorities in India are as follows:
Regulatory authorities governing social media can be broadly divided under two heads

A. Statutory/State authorities
B. Non statutory authorities
   i. Internet Service Providers
   ii. Social Media Agencies

A. Statutory/State Authorities
As social media mischief creates law and order challenge, therefore, both central and state governments have the power to frame rules for social media because power to frame rules for criminal law is mentioned in concurrent list of Constitution. However no such rule pertaining to social media has yet been framed by any govt. in India. A guideline on ‘The Framework and Guidelines for Use of Social Media for Government Organization’s issued by Ministry of Communications & Information Technology, Government of India caters strictly to govt. organizations and general public are not to follow them.

Section 69 A of the Information Technology Act grants power to the Central Government to issue directions to block public access of any information through any computer resource on similar grounds. Additionally, Computer Emergency Response Team (CERT-In) has been established by virtue of section 70 B of the IT Act. It says that Central Government shall provide the agency with a Director General and such other officers and employees as may be prescribed. The Indian Computer Emergency Response Team serve as the national agency for performing these functions:
   (a) collection, analysis and dissemination of information on cyber incidents
   (b) forecast and alerts of cyber security incidents
   (c) emergency measures for handling cyber security incidents
   (d) coordination of cyber incidents response activities
   (e) issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents

121 The guidelines stand as the first attempt to provide a legal framework that governs social media in India. These guidelines however cater strictly to Governmental Organizations which means only the employees of the government and not the general public is to follow them.
(f) such other functions relating to cyber security as may be prescribed

For carrying out these functions effectively the agency may call for information and give direction to the service providers, intermediaries, data centres, body corporate and any other person.

Further, Central Government or a State Government or any of its officer specially authorised by the Central Government or the State Government, as the case may be, is satisfied that it is necessary or expedient to do 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, it may, direct any agency of the appropriate Government to intercept, monitor or decrypt any information transmitted received or stored through any computer resource.\(^{122}\) IT Act makes it a mandatory duty for the intermediaries to assist the govt in such matters.

But in the absence of any special law, these authorities find it hard to act on offences committed over social media. CERT-In which is working exceptionally well in the tasks for which it has been created by the govt. of India has less personnel as compared to CERT-US. There is very less budgetary allocation for its functioning.

Cyber cells\(^ {123}\) which have been established in India, having regard to increasing number of cyber crimes, have jurisdiction to take cognizance of offences relating to hacking, child pornography, cyber stalking, denial of service attack, virus dissemination, software piracy, IRC Crime, Credit card fraud, net extortion and internet banking frauds. Social media platform can be used for committing these crimes and cyber cells can take

---

\(^{122}\) Section 69 A of the IT Act, 2000

\(^{123}\) Various cyber crimes cells have been established in India in different states. Mumbai, Lucknow, Bangalore, Chennai, Hyderabad, New Delhi, Haryana, Bihar, West Bengal etc. are the cities in which cyber cells have been established. In those cities where cyber cells are not created a senior police official is in charge of cyber crime matters.
cognizance of it. The cyber cells are confined to investigatory aspects of social media mischief. There is hardly anything to suggest that they have preventive powers.

To monitor the activities on social media networks the Mumbai police have established a 'social media lab.' The project is supported by the National Association of Software and Services Companies (NASSCOM) and is funded by Reliance Foundation. As per the news reports the lab will have police personnel along with social media experts. According to the lab experts, since it will not be possible to monitor each and every comment, the department can single out netizens with criminal records, anti-social and anti-national agendas and track their online activities. Bangalore Police has also planned to establish the social media labs to monitor activities on social media pages. The U.P. Govt. has also established two 'laboratories' to monitor content on social media sites such as Facebook and Twitter, and help the police assess situations pro-actively, particularly during a crisis.

Apart from the government there are various other statutory bodies which may curtail the freedom of social media users. For example Election Commission of India has issued instructions for social media usage by the candidates during 16th Lok Sabha elections in India.

124 Various cyber cells established in India provides for online filing of cases or they can be directly approached. Procedure for filing a complaint is mentioned on their website. For example the web page of cyber cell lucknow explicitly mentions 'how to report'. See; <http://cybercrimecelllucknow.org/How_to_Report.html> (accessed on 02 Dec. 2014)


Underlining the need to regulate the social media the Press Council of India in its press release resolved for more power accredituation. It even demanded for an adoption of a wider name in the form of the ‘Media Council of India’ from the present name of ‘Press Council of India’. In its press release by citing example of mischief caused by social media in north east press council stated that “......claim of the broadcast media for self-regulation is futile and meaningless, because self-regulation is an oxymoron. All social activity has to be regulated. Regulation is different from control. In control, there is no freedom, while in regulation, there is freedom but it is subject to reasonable restrictions in the public interest. The Press Council is in favour of regulation and not control, and this regulation should be by an independent statutory authority like the Press Council of India and not the government.”\(^\text{129}\)

**B. Non Statutory Authorities**

Non statutory authorities are the first to play a crucial role in the regulation of social media. Social media companies and Internet service providers have primary role in regulating the content on the internet.

i. **Social Media Agencies**

Private companies that run social media sites and search engines have the dominant role in what gets communicated in cyberspace. These companies often employ “terms of service” that censor a broad range of constitutionally protected speech. For e.g. Instagram released an updated version of its online terms of service and privacy policy in Dec. 2012. The updated Terms would have allowed Instagram to use a user’s likeness and photographs in advertisements without compensation. There was a strong backlash from users over the updated Terms, which ultimately led to Instagram apologizing to its users for the advertisement-related changes, and reverting to its previous language regarding

\(^{129}\) Press Council of India, ‘PCI resolves for more powers and conversion to Media Council of India’ (Press Release, 28 August 2012) <http://presscouncil.nic.in/OldWebsite/Resolution.pdf> accessed on 17 September 2013
advertisements.¹³⁰ Instagram’s changes to its Terms, and subsequent reversal, are reminders of how monetizing social media services are often a difficult balancing act.

Every social networking site provides for certain safeguards to prohibit unwarranted use of its services.¹³¹ Facebook’s “Statement of Rights and Responsibilities” provides: “You will not post content that: is hate speech, threatening, or pornographic; incites violence; or contains nudity or graphic or gratuitous violence.”¹³² There are few categories of speeches which in the Facebook itself which is not protected by the First Amendment of US Constitution. But there is no judicial determination of illegality – just the best guess of Facebook’s censors. Facebook’s internal appeals process is mysterious at best.¹³³

ii. Internet Service Providers

Internet Service Providers (ISPs) have stepped in to censoring web contents either compelled by the laws or, on their own accord. For example, in China ISPs are forced to monitor the users and report right away to the government in case any misuse of the internet takes place. While public authorities in many countries do not divulge into such censorship directly, they put in tacit pressure on the ISPs. The establishment of the Internet Watch Foundation (IWF) in UK, caused by implicit pressure from the


¹³¹ For example facebook provides for reporting a problem, blocking, App Passwords, Trusted contacts and trusted browsers and privacy managing services. See; Facebook, ‘Data Policy’ (Facebook, 30 January 2015) <https://www.facebook.com/full_data_use_policy> accessed on 16 Feb. 2015


Metropolitan Police is an apt example of such implicit pressure. In Sweden, though, the ISPs have proactively taken initiatives to control access to certain websites. While such practices by ISPs remain a matter of serious concern with regard to their capability of deciding which content is offensive, and hence, would require censorship. The role of the State in various countries vis-a-vis regulating cyberspace too need to be thoroughly analyzed.

- **Liability of ISPs**

The concept of intermediary liability has surfaced due to the distinctive architecture of the internet. Exchange of information on the internet takes place by sending packets of data over privately-owned networks, and this process is made feasible by the infrastructural support provided by intermediaries. Legal issues may arise because of the distribution of content or the provision of services on the Internet. While the vast majority of activities on Internet intermediary platforms are lawful, illegal activities raise questions of liability. Since it is difficult both to trace the actual perpetrators and to curb the instantaneous circulation of unlawful content, many states have found it convenient and effective to impose liability on intermediaries, which host, transmit and locate such information.

---


137 Sec. 79 of the IT Act deals with exemption from liability of intermediary in certain cases. According to section 2 (w) of the Act "Intermediary" with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes.

In India, the government in its attempt to regulate content on the internet has put tacit pressure on intermediaries to monitor and screen content. It resulted into private, invisible censorship and severely endangered the exercise of right to freedom of speech and expression. Even though, similar on the line of other nations, India has also incorporated a safe harbour provision in order to limit ISPs liability but it has been of little help. The statutes addressing the issue of intermediary liability is the Information Technology Act (as amended in 2008) & the Copyright Act (as amended in 2012). Sec. 79 of the Information Technology Act is a broad-based definition which provides for conditions under which exemption would be provided to intermediaries. However its effectiveness in providing immunity to intermediaries has been hampered by failure to acknowledge and provide for the functional differences of the intermediaries. Another problem is that in the matter relating to due diligence requirement or other obligations, IT Act treats different kind of intermediaries as equal. There seems no logic behind treating them as equal when various countries are making distinction between different classes of intermediaries.

IT Act also provides that ISPs shall be liable for huge compensation if they fail to remove the prohibited content. There are several undefined categories for which intermediaries are left alone to exercise their wisdom as to whether the content violates statutory terms. In order to escape the risk of incurring liability, ISPs often block more content than required. The chilling effects of these rules can affect the creation of innovative expressions among the users.

139 Microsoft, Yahoo, Google, Facebook and other Internet companies have been named in separate civil and criminal suits filed in Delhi courts over alleged objectionable religious and other content on their websites. The government allowed the court to prosecute the Internet companies under various Indian laws in the criminal case. The criminal suit was filed against the Internet companies in a separate court in Delhi, by newspaper editor Vinay Rai. Google and some others appealed the criminal court's decision before the Delhi High Court. In the civil court, Google agreed to pull down the content cited as objectionable. For details see John Ribeiro, ‘Court Drops Google India From Objectionable Content Case’ (PC World, 13 April 2012) <http://www.pcworld.com/article/253712/court_drops_google_india_from_objectionable_content_case.html> accessed on 20 Aug 2014

The legislative ambiguities as discussed above, coupled with the onerous obligations imposed on intermediaries, threaten to defeat the purpose of providing safe harbour protection. While it is acceptable that the unique architecture of the internet necessitates intermediary liability for control of unlawful activity, this argument has to accommodate the fact that intermediaries also play an indispensable function in ensuring free flow of ideas and information on the internet, and thus, require some protection for liability. If the same would not be provided to intermediaries they are likely to reduce this free flow of ideas and information to avoid the risk of exposure to liability. For instance, if an intermediary is notified for hosting obscene content, then even if the content is not actually obscene or even if the complaint seems dubious, the intermediary will still err on the side of caution and remove the content, in order to shield itself from potential liability.¹⁴¹

### 2.2.3 MODES OF REGULATION

The regulatory authorities exercises two methods in regulating internet and social media websites-

A. Content Regulation and

B. Access Regulation

### A. Content Regulation

Content regulation of the internet is a debatable issue of which both govt. and internet users are concerned about. Govt. takes initiatives to take down the objectionable content from social media websites when it finds the content against the laws of state. ISPs at the instance of govt. put filtering software on their servers to restrict the distribution of certain kinds of material over the Internet. Terminate TCP (Transmission Control Protocol) is the mechanism which detects certain number of controversial keywords.

¹⁴¹ Pritika Rai Advani, ‘Intermediary Liability in India’ (2013)14 Economics & Political weekly 50
This affects all TCP-based protocols such as HTTP, FTP and POP, but Search engine results pages are more likely to be censored.

The concept of “content” in cyberspace includes everything that is created and would apply, to every websites and weblogs. The wide scope of the word “content” provides a difficulty for governments when considering content regulation on the Net. The move of the govt. to regulate internet has been debated as supporters claim that state has a role to prohibit harmful content while critics argue believe that the individual must have the right to choose.

The Govt. of India issued a regulatory order seeking the removal of objectionable content. The websites such as Google, Facebook, YouTube and Yahoo were asked to evolve a mechanism to filter such “inflammatory” and “defamatory” content that could create social tension. The Lucknow bench of the Allahabad High Court in response to a PIL has asked the Centre to ensure that web service providers, social network sites and search engines like Yahoo, Facebook, Twitter and Google must make available grievance redressal cell on their pages, which is mandatory under the Information Technology guidelines. The court asked the petitioner to submit representation intimating the Central government about his grievances and directed the Centre to address them within three months. The order was passed by a division bench comprising Justice Uma Nath Singh and Justice VK Dixit on a petition seeking implementation of Rules 3 and 11 of the Information Technology (Intermediary Guidelines) Rules 2011.

142 In this case Yahoo filed a written statement advancing the facts that „Yahoo is not a social networking site” and facebook and twitter both advocated in its protection that they are only the medium. They argued that „we are only intermediaries providing a mechanism for people to share their views. If something seems objectionable the user should be held liable in accordance with law rather than the machinery working as medium. Freedom of speech and expression is possessed by the people (user) only and therefore, it must be curtailed/regulated against the people (user) only and not against the medium. See; Sandeep Joshi, ‘Government warns social websites over objectionable content’ The Hindu (New Delhi, 06 Dec. 2011) 1

Social media webs itself provides mechanism to regulate the contents of their page. For example

- Facebook Statement of Rights and Responsibilities says: "You will not post content that: is hateful, threatening, or pornographic; incites violence; or contains nudity or graphic or gratuitous violence", "You will not use Facebook to do anything unlawful, misleading, malicious, or discriminatory", "We can remove any content or information you post on Facebook if we believe that it violates this Statement".¹⁴⁴

- Twitter: The Twitter Terms of Service state: "We reserve the right at all times (but will not have an obligation) to remove or refuse to distribute any Content on the Services and to terminate users or reclaim usernames" and "We reserve the right to remove Content alleged to be [copyright] infringing without prior notice and at our sole discretion" ¹⁴⁵

- YouTube Terms of Service include the statements: "YouTube reserves the right to decide whether Content violates these Terms of Service for reasons other than copyright infringement, such as, but not limited to, pornography, obscenity, or excessive length. YouTube may at any time, without prior notice and in its sole discretion, remove such Content and/or terminate a user's account for submitting such material in violation of these Terms of Service", "YouTube will remove all Content if properly notified that such Content infringes on another's intellectual property rights", and "YouTube reserves the right to remove Content without prior notice".¹⁴⁶


B. Access Regulation

Access regulation is a broader term which connotes different notions of preventing access to internet. It may be partially allowed access or completely prohibited access. Access regulation is related to state directed implementation of national content filtering schemes and blocking technologies affecting internet access. State and ISPs uses various methods such as take down, result removal or technical blocking to give effect to state mandated filtering.

Types of access regulation:

- **Internet Protocol (IP) address blocking**: through this mechanism access to a certain IP address is denied. If the web site which has to be blocked is hosted in a shared hosting server, every website on the same server will be blocked. It affects IP-based protocols such as HTTP, FTP and POP. However this mechanism can be avoided by using proxies that have access to the target websites, but proxies can also be jammed or blocked.

- **Network disconnection**: A technically simpler method of access regulation is to completely cut off all routers, by turning off machines & pulling out cables. This method immediately disconnects all the machines from internet. It appears to have been the case on 27/28 January 2011 during the 2011 Egyptian protests, in what has been widely described as an "unprecedented" internet block. Full blocks also occurred in Myanmar/Burma in 2007,147 Libya in 2011,148 and Syria during the Syrian civil war.

- **Portal censorship and search result removal**: Search engines and major internet portals may exclude those web sites which they would ordinarily include in their search results. This renders a site invisible to people who do not know where to

---


Any removal by search engines under this method amounts to censorship. Sometimes this method is adopted to satisfy a legal requirement, other times it is purely at the discretion of the portal. For example Google.de and Google.fr removed Neo-Nazi and other listings in compliance with German and French law.

The first instance of access blocking can be traced to China, wherein, access to a list of IP addresses, keywords, and domains is actively blocked. This list – prepared by the government – is passed to individual Internet Service Providers (ISP) for blocking access to a particular web resource. In China, the government has cracked down on social media platforms blocking sites such as Facebook and Twitter. The authorities have introduced their own social media platform, Weibo, which is a highly controlled micro-blogging website. It allows China's citizens to keep pace with the growing world of the internet, while ensuring its content is regulated. This paves the way for them to filter the news and produce it in their own colour. China has an elaborate mechanism in place to effect censorship known as “Great Firewall of China” and officially as “Golden Shield Project”.

### 2.3 CONCLUSIONS

As discussed earlier in this chapter the problems created by social media are mostly individualistic per se except hate speech and pornography which affects society at large. At present these issues are being addressed with different set of laws for example IP Issues are governed by Trade Mark Act, Copyright Act etc. and rest are governed by other statutes. In social media regulation these issues can be effectively addressed taking into consideration the existing laws. But in relation to those problems which are being governed by Information Technology Act, it would be necessary to redraft the IT laws including regulations. IT Rules says that ISPs are required to remove the prohibited content within thirty six hours when it receives notice. They have been given power to block the access of the concerned user. The concerned user is not even notified about the removal of his contents. The intermediary is neither required to hear the third party of the information before or after the removal of contents, no under an obligation to provide a
reasoned decision for the take down notice. While exercise of this power is necessary by the ISPs but in the absence of any judicious mechanism it also encourages privately administered injunctions to censor free expression.

Legal regulation of these conflicts is possible by proper legislative efforts in which the following areas may be covered in order to formulate a legal policy.

a. Rights, duties and responsibilities of social media owner agencies/companies

In order to regulate the social media webs, it is necessary that the social media agencies should first start introspecting their functioning. There is a pressing need to clearly mark their rights, duties and responsibilities towards users in specific and society at large. At present, most social media agencies are regulating their functioning voluntarily and which varies from agency to agency. To bring harmony and consistency in the rules it is necessary that the functioning of social media should be regulated through law. Rights, duties and responsibilities of agencies should primarily ensure and protect the interest of the user first of all. Secondly, it must also have preventive mechanism to stop the potential victimization of user in case of any serious happening or mishappening. The agencies ought to also focus on development of such specification in the application which may not be highly invasive in terms of user data and which may have the potential of threatening/jeopardizing the user`s interest.

b. Rights, duties and responsibilities of the social media users

Rights, duties and responsibilities of social media user should also broadly focus on ensuring peace and harmony in the society i.e. the application should not have such features which may be misused by the user to create ruckus/disharmony in the society. This is particularly in case of those offences which have the potential of unleashing mass scale violence like hatred or communal harmony in the society. Though rights, duties and responsibilities of the social media users are governed through different set of laws yet the internal inconsistency in these laws and their openness towards changing dimensions of information technology is highly questionable. Duties and responsibilities of the users varying from place to
place highlight the challenging task of regulation. Need for an international body
to govern the social media behavior is apparent.

c. Rights, duties and responsibilities of Internet Service Providers (ISPs)
Functioning of ISPs in most countries is well regulated. As discussed earlier in the
chapter, in India Information Technology Act clearly set out the rights, duties and
responsibilities of the ISPs. However, various concerns have been raised which
needed to be addressed. Effectiveness in providing immunity to intermediaries
may be hampered by its failure to acknowledge and provide for the functional
differences of the intermediaries. Laws governing ISPs in every country is
entirely different in nature which paves way for free and independent functioning
of internet in a particular country. In this case also there is a pressing need to have
an international understanding regarding rights, duties and responsibilities of the
ISPs.

d. Creation of statutory regulatory bodies and devising their powers, functions and
responsibilities
As discussed above, the approach of govt. in regulating the social media websites
is often seen as an attempt to curtail individual freedom of expression on the
internet. In order to bring rationality and reasonableness it is necessary to have a
dedicated body responsible for governing social media. The govt. should
formulate a proper strategy, mechanism for effectively dealing with the cases in
which there is a large scale mischief spread over a considerable part of the
territory. This may lead to effectively handling those situations which occurred in
north eastern mass exodus.
The cyber cells are confined to only investigatory aspects of social media
problems. Therefore there is a need to have a designated body which is totally
devoted to regulate the functioning of social media. Social media labs, which have
been established in few cities in India, can be a viable option to monitor the online
activities. Social media labs play a preventive role in controlling the social media
mischief. However, the rights and duties of the body should be well formulated in order to avoid any uncomfortable situation.

e. Rights, duties and responsibilities of application developers on social media

A legal, moral and ethical code should be devised for social media application developers and there should be a body for granting approval to properly devised social media applications. A free and unhindered growth of social media application which is being launched in thousands everyday are creating massive problems in public domain. So there should be a check on launching social media application particularly keeping in view the interest of society/community/public at large. Testing and approval of social media application for the purposes of its launching in public domain is becoming essential day by day.

It can also be concluded that hate materials on internet are the biggest problem today and it should be prohibited on a priority basis. Organizations such as INACH and national governments should unite to work against cyber hate. The private public partnership will help in the prevention of cyber hate. Though this task will take a longer time, it is possible and the need of the hour.