International Journal of Multidisciplinary Research and Development
Online ISSN: 2349-4182, Print ISSN: 2349-5979, Impact Factor: RJIF 5.72
www.allsubjectjournal.com
Volume 4; Issue 5; May 2017; Page No. 132-142

Social networking sites and data protection: A critical study

Ashok Kumar Kasaudhan

Assistant Professor, School of Law, Galgotias University, Gautam Buddh Nagar, Greater Noida, Uttar Pradesh, India

Abstract
This paper attempts to analyse as to whether legislative framework relating to data Protection which regulates the various aspects of social networking is sufficient or not. Nowadays social media has become an important part of people's interactive life. Popularity of mode of interaction lies in the fact that it has become preferred mode of interaction among more than half a billion population of the world. It has its reach among all the age groups of netizens. There are multifaceted role of social media in one's life such as texting, posting views and pictures, remaining in touch with friends and clients etc. Its popularity is increasing day by day and now it has become an important part of native's life.

Keywords: social networking, data protection, social media

Introduction

Nowadays social media has become an important part of people's interactive life. Popularity of mode of interaction lies in the fact that it has become preferred mode of interaction among more than half a billion population of the world. It has its reach among all the age groups of netizens. There are multifaceted role of social media in one's life such as texting, posting views and pictures, remaining in touch with friends and clients etc. Its popularity is increasing day by day and now it has become an important part of natives life.

Social network websites is Online Platform for Social Networking which allows users to build connections and relationships with other Internet users. It provide a virtual platform which is usually used to keep in touch with friends, make new contacts and find people with similar interests and ideas and also enable users to interact and exchange information about themselves, use blogs and private messaging to communicate with friends, others and sometimes even the world at large. By the help Social networking sites one can contact with his friends, colleagues relatives, and share media like music, photos and enjoying the communities of like-minded. Website functions like an online community of Internet users. Depending on the website, many of these online community members share a common interest in hobbies, religion or politics.

Kinds of social networking websites

There are many types of social networking website available online. Each& every Social networking platform has its own Policy and setting for privacy some are simple and some are more complicated than others. On the basis of the nature and utility they can be classified into following:-

Social connection network.

This type of networking allows users to create accounts on social networking Websites and to provide detailed individual personal information on profile of such Social Networking Accounts. These accounts help other users in establishing social relationships in cyber world. There are various platforms for this purpose such as Facebook, Friendster etc. These social networking sites are generally used to share certain information such as hobby, ideology, date of birth, interests, academic qualification and various other personal choices keeping in view the aim and objective of particular websites. Besides this there are certain information which can be shared even though they are not authorized contacts.

Microblogging Networks

These websites or programmed for special purpose and they facilitate users to update their status quickly. These types of sites are specially meant for professionals as they do not have sufficient time to communicate with their fellows and employees in leisure. Such as twitter enables short updates of certain news stuffs. These websites are meant for broad casting information very quickly in public domain; however at certain occasion's privacy settings are there which restricts the access up to certain domain to some extent.

Location Networks

There are certain location based networks and they are part and parcel of location based service. This has been become possible because of Global Positioning system (GPS), which are used in tracking user's location and are much effective and at par with the capacities of World Wide Web. Along with GPS it is also enabled with few special features such as instant messaging. Earlier location based networks were not prevalent but after but once GPS came into existence location networks became popular and are being used frequently. These are also very helpful in positioning of various mode of communication such as Railway, Aircraft, buses etc. Many a times these networks are used as a medium of interaction with other social networks

Multimedia sharing networks

This is different type of social media platform which is used for sharing certain audio-visual stuffs such as songs, music, photographs, videos etc. These networks reflect dual nature such as sometimes they behave as a social network based pattern and sometimes they behave as content hubs. YouTube, Instagram etc. are its biggest example.

Shared-interest or dating networks

Some social networks are built for dating between man and women of a common feature and common priority list based on personal instincts. Although it looks like social networking site but in reality it is not true and it is tilted towards individuals. This is meant for person with identical hobbies, backgrounds, political affinity, sexual instincts, and other common but peculiar feature. Major Websites providing these types of services are Tinder, Matchily and TruklyMadly etc.

Professional Networking

This type of networks specially focuses on career related aspects and here professional of various fields are supposed to exchange views, research, editorials etc. With other professionals. Here professionals communicate and interact among themselves and in this way these websites provide platform for views and convictions of various professional at one place. Such platform includes LinkedIn, Academia.edu etc.

Educational Networking

This type of networking is specifically meant for students and provides them a common platform to discuss and debate on academic issues. In online medium students happens to collaborate with other students on academic topics and sometimes they also conduct research at school level. It enables the students to interact and ask questions from academicians directly. With the advancement of technology these websites have become more and more popular among students as they provide better atmosphere to the students.

Due to increasing in numbers of users of social media most social networks websites combine feature of more than one of these types of social networking Site, and the focus to target the interest and demand of present as well as new user of social networking. For example Facebook it has combine feature of many other Social networking Sites like, it has the following and follower feature which is very much similar to that of twitter, FB Messenger for chatting, similar to Instagram it has a Moment App for sharing Pictures, now Facebook has also included the location base networking features.

Privacy risk in social media

The use of internet based social networking sites has pervaded urban Indian Lifestyle almost completely. There is no domain of life that is uninfluenced by the spawning of social networking platforms. If Facebook were a country, it would be the third largest country in the world.

The use of this social networking platform is not limited to the social sphere it transcended from finding a job to finding Spouse.

Social networking sites and associated privacy risk is one of the most debated topic nowadays as participation in such sites has increased dramatically. A number of journals and articles come up with this issue that how the increase in the usage of social networking sites is leading to various online crimes.

The evolution of new technologies and growing popularity of social media like Facebook and Twitter, we are witnessing increasing threat to the Privacy and information security. Which give rise to two distinct kinds of risk to privacy? The first set of concerns relates to the disclosure of personal information by the users of Social Networking themselves and the second set of concerns, on the other hand, relates to the posting of personal information about such user by other people, including the possibility of other people altering someone's personal information. Therefore, the privacy concern in this area is obvious. Even from an economic perspective the robustness of this market can only be preserved if the integrity of data is protected.

"Maintaining privacy on social Media is much like hanging all your dirty clothes in a balcony of your house and then asking only your friends to look it. While it's possible to avoid sharing your life's story with the entire world, it takes a lot of effort and is often contrary to the goals of the services you use".

The notable issue that, these Social Networking services are free, Social Networking services Provider do not charge any price for providing these services, because they are selling access to *you* and the use of such websites provides them with substantial amount of data. This data is mostly of sensitive and very personal in nature. This data could in fact put a person's entire life at risk even a degree of interaction that is carried out in this space.

Social networking sites rely on a communication building connections, which encourages the user to provide a certain amount of information, people who were unaware of the risk and threat to their privacy share lots of personal and sensitive information about them on the social media Sites. Which provide, opportunity to various cyber criminals to misuse such information to get undue advantages and thereby causing acute harm and breach of Right to Privacy on the users whose information is so used? Therefore online site can be quite useful and are extremely popular, it is important to remember that sharing too much information online can be risky.

Privacy concerns are especially acute in the case of multimedia collections, as they could reveal much of the user's personal and social environment. Due to this high penetration of smart phones with photo and video creation and sharing opportunities, the amount of personal content available online is has been increasing rapidly in the last years. The easy and rapid Sharing of personal content such as picture and video on Social Media, arise new privacy concerns due to their context revealing details about the physical and social context of the subject. Therefore, the increasing use of social media and the growing amount of online expose of personal content such as picture and video today had resulted in high level of security and privacy risk.

Criminals may use social networks to connect with potential victims. There are three water degree of security risk arising from the use of social media: 1) Malware infection, 2) Data leakage, 3). Unwilling attack participation.

Privacy in social networking arena requires a compact understanding as to what really it does mean. It largely depends upon the intent of sharing individual. When privacy issues relating to social media are contemplated, there are three points which must be taken into consideration.

1. The intention behind the Sharing of information and the expectation that it will remain private. A person who willingly posts information on a social networking site for others to view cannot assume it is private because he intent is to share that information.
2. When an individual uses privacy settings to prevent most users from viewing his or her information, the user has an expectation that this information will remain private but the grave facts that anything they post online is public and

cannot be assumed private when an individual shares information on a social networking site, he or she is sharing that information with the rest of the world even if the intent was to share with only a select group of people.

3. People react and become sensitive about their privacy later when they feel that they are being exposed [1].

The Challenge in providing privacy protection social networking platforms that, personal information of particular person is not in control of the same person in all circumstances for example, the user may be tagged in picture uploaded by another in this circumstances the person to whom information pertains has no control over the visiting.

Thus, the availability of personal information on social networking website also provides an opportunity to identity thieves, scam artists, debt collectors and, stalkers to misuse the information that people themselves shave voluntarily provide.

It is easy to steal personal and other information about individual From Social networking sites. The personal information available on Social Networking Sites can be used to conduct the social engineering attack additionally because of popularity of these sites attacker may use them to distribute malicious code and this is a critical factor for individual as well as corporations.

Social network with hundreds of millions of user, are logically the target of cybercrimes. Criminals are increasingly using social networking site to perpetrate identity fraud for financial gain or espionage. Where predators usually target children and females user of social networking site.

However, many people besides friends and acquaintances are interested in the information which people usually post on social networking Sites. Identity thieves, scam artists, debt collectors, stalkers, and corporations looking for a market advantage are using social networks to gather information about consumers. Companies that operate social networks are themselves collecting a variety of data about their users, both to personalize the services for the users and to sell it to advertisers.

This section discusses some of the typical scams and devices used to defraud consumers on social networks. Fraud may involve more than one of the techniques described below. Some types of fraud may not be described here.

Identity Theft

Identity Theft occurs when someone, without your knowledge, acquires a piece of your personal information and uses it to commit fraud.

Identity theft is a crime used to refer to fraud that involves someone pretending to be someone else in order to steal money or get other benefits. The term is relatively new and is actually a misnomer, since it is not inherently possible to steal an identity, only to use it. The person whose identity is used can suffer various consequences when he or she is held responsible for the perpetrator's actions. In many countries specific laws make it a crime to use another person's identity for personal gain. Identity theft is somewhat different from identity fraud, which is related to the usage of a false identity' to commit fraud. Identity theft can be divided into two broad categories: 1. Application fraud 2. Account takeover.

Application Fraud

Application fraud happens when a criminal uses stolen or fake documents to open an account in someone else's name. Criminals may try to steal documents such as utility bills and bank statements to build up useful personal information. On the other hand they may create counterfeit documents.

Account Takeover

Account takeover happens when a criminal tries to take over another person's account, first by gathering information about the intended victim, then contacting their card issuer masquerading as the genuine cardholder, and asking for mail to be redirected to a new address. The criminal then reports the card lost and asks for a replacement to be sent

Identity thieves use an individual's personal information to pretend to be them, often for financial gain. The information users post about themselves on social networks may make it possible for an identity thief to gather enough information to steal an identity. In 2009, researchers at Carnegie University Mellon published a study showing that it is possible to predict most and sometimes all of an individual's 9-digit Social Security number using information gleaned from social networks and online databases.

Information often targeted by identity thieves includes:

- Passwords
- Bank account information
- Credit card numbers
- Information stored on a user's computer such as contacts
- Access to the user's computer without his or her consent (for example, through malware)
- Social Security numbers. Remember that the key to identity theft is the Social Security number. Never provide a Social Security number through a social networking service. Some fraud techniques to watch out for include:

Illegitimate third-party applications [2]

These rogue applications may appear similar to other third-party applications but are designed specifically to gather information. This information may be sold to marketers but could also be useful in committing identity theft. These applications may appear as games, quizzes or questionnaires in the format of "What Kind of Famous Person Are You?"

False Connection Requests

Scammers may create fake accounts on social networks and then solicit others to connect with them. These fake accounts may use the names of real people, including acquaintances, or may be entirely imaginary. Once the connection request is accepted, a scammer may be able to see restricted and private information on a user's profile.

Hacking

Hacking unauthorised access to a computer and a first to access the whole or in part of computer system without permission hackers worldwide attempts to hack into remote computer system for multiple purpose like eavesdropping, data theft, fraud, destruction of data, causing damage to

[1] Dianne m. timm & carolyn j. duven, "privacy and social networking sites" 24, wiley interscience, 2008

[2] Social Networking Privacy: How to be Safe, Secure and Social available at https://www.privacyrights.org/social-networking-privacy-how-be-safe-secure-and-social accessed on 28/03/2016

computer system, or for mere pleasure or for of personal satisfaction.

The meaning of the term hacking and evolved over time applied somewhat wary are too complex legal and illegal activities ranging from legitimate creative programming technique illicit lock -picking and manipulation of worldwide phone or computer system. At the basic level hackers are considered to be a learner and explorer who want to help rather than cause damage and warfare have very high standard. A hacker may not indulging vandalising or maliciously destroying data, or stealing date of any kind. But the term hacking is required to well-meaning today and had them invariably means cyber burglar or Randall, an individual or a group who believe in causing malicious harm when network computer by Steve information like passwords and credit card numbers name and addresses, financial information email account information for the ISP, and in short anything stored on computer.

There are several cases registered or unregistered relating to hacking in India. Examples are ZeeTV.com, Goznextjob.com, etc. and a notorious group of Pakistan hack hackers called GeForce during 2001 who had many websites opinion organisation such as Indian science Congress, Asian age newspaper, National research Centre, agriculture University of Maharashtra, IIM (Ahmadabad), Etc. that in 2002, the website of Assam tourism department was hacked by unknown hackers here the hackers are replaced most of the photograph to tourism interest with pornographies.

Perhaps, the most shocking instant adding India is, when the 15-year-old American boy, hacked into the Mumbai-based, Bhabha Atomic Research Centre (BARC) computer network soon after the Pokhran Nuclear Test.

Hacking, result in a violation of individual's privacy and therefore it has been made a punishable offence under section 66 of information technology act 2000.

Cyber Stalking [3]

Cyber stalking is a crime in which the attacker harasses a victim using electronic communication, such as email or instant message, or messages posted to a website or through social networking sites or a discussion group. Cyber stacker relies upon anonymity enabled by the Internet to allow him to stalk his victim without being detected. Cyber stacking messages differ from ordinary spam in that the cyber stalker targets a specific victim's frequent and threatening messages while the spammer targets multitude of recipient with simply annoying messages. Stocking has typically been defined as involving ' repeated harassing or threatening behaviour". The goal of the traditional stalker is to exert control by instilling fear into a victim.

While cyber bullying and cyber harassment may damage an individual's reputation livelihood, cyber stacking is more likely to result in serve an immediate emotional or physical harm. Cyber stalking began with email messages most often followed to a message board and for messages was restrict wedding chat. In some cases cyber stalking develops from a real-world Stalking incident and continues over the Internet through social networking sites however cyber stalking is also sometimes followed by is talking in physical world with all its attendant danger stacking and harassment are malicious activity directed at a particular person. They may or may not be deemed criminal activities, depending on the jurisdiction. But when these activities are committed by a computer, all duration may not be able to prosecute them. This is a serious challenge to every domestic criminal law even if it is updated to cover cybercrime.

Cyber Bullying

Passing of derogatory or offensive remark about one's gender race religion believe nationality and sexual orientation, under the purview of cyber bullying which is a common type of cybercrime all the over world. The term cyber bullying typically refer to online abuse stop the term bullying in the physical world tend to describe conduct that occur when someone uses for of coercion to control and person. If such bullying is done on online domain then it will be termed as the cyber bullying. Such behaviour is seen to be habitual Can involve tormenting, threatening, harassing, humiliating, embarrassing or otherwise targeting a victim.

Privacy policies offered by social networking sites

A social network's privacy policy is rules available on most of the Social Networking website, which explains in detail how the social networking Site will collect and use information provided by the user and also the information about people who visit the site.

Social networking sites vary in the levels of privacy offered and required. For instance Facebook, currently the king of the social network sites, encourages its users to use their real names and upload personal information on their profile page. Such as profile picture, birthday date, addresses, Contact numbers and more intimate details such as interests, hobbies, relationship status and sexual preference. After one posting all that on his/hers profile page, one can imagine how narrow user's privacy actually becomes.

Mostly every big social networking site had provided their privacy policies and controls. However, these policies and settings are dense and complicated for a common user. Many people skip over the privacy policy when joining a social network. Therefore, in many areas such Privacy Policy fails to provide effective protection.

Usually, Social networking site set a particular default privacy setting which allow maximum access unless they are actively changed. This approach places large number of users given the fact the user is not effectively informs publication of falling to the actively changed sitting. Some of the information users provide to a social network is readily apparent such as providing a birth date in order to create a new account.

Sometimes, the social networking Site may collect information of users online Behaviour "invisibly" by the means of tracking activity of users within the social network, Such as what links/page they likes on and even which websites they visit after leaving the social networking site.

Most social networking site in response to privacy breach issue, takes recourse to consent of reasonable who agrees to the term for the sharing and using of information. However mainly jurisdictions have taken a progressive view in analysing the manner in which such information is presented

[3] Cyber-stalking: the Regulation of Harassment on the Internet By Louise Ellison and Yaman Akdeniz available at http://www.demonish.com/cracker/1431329602_58a7349092/stalking_article.pdf. accessed on 29/03/2016

to the user. In other words, consent is said to valid only when such information is lawful, real and unambiguous and provided in an understandable manner.

The most common problem that is faced in deciding the issue of breach of Privacy is the actual and proper interpretation of the term "knowledge& information of meaningful consent". Further, some of this platform retain it information for inordinately long period of time, thereby creating privacy risk. Data security to prevent breach is one of the most urgent need of social networking market to preserve consumer confidence.

Thus Sharing can be fun, productive and rewarding. But social media users, who don't exercise reasonable caution and take the time to learn the data-use policies of each site they post to, may find they are sharing more than they mean to or are comfortable with. This is why many social networks provided privacy Polices for data collection and data retention and also offer ways to control how much you share and who you share it with.

Social networking and privacy issues [4]

Social networking is the interaction of people through social networking websites. Some of the most common social networking sites are Facebook, Orkut, LinkedIn and Friendster. Social networking sites have become popular means of connecting people to people to maintain contacts and to establish business contacts. The users of social networking sites generally post information regarding their birth dates, gender, place of residence and work, their educational qualifications, details about schooling, their hobbies, interests, marital status etc. Which can clearly give rise to privacy issues?

Accordingly Social networking sites such as Facebook provide security settings to protect privacy of user's accounts. For example user of Facebook can use settings which make their profile visible only to their friends and can block who can view the pictures or messages on their profiles. These securities setting enable users to make available information to their friends with whom the user wants to share the information.

However social networking sites use click-wrap agreement. Once the user has clicked on 'I agree', he had accepted the terms and conditions of agreement and would likely to have waived some of his privacy rights depending upon contracts. The terms and conditions of click-wrap agreement are generally difficult to read and users tend to click 'I accept' without have read anything.

However social networking sites may not provide sufficient security measures as there are no SSL logins provided (secure socket layer). This makes it easier for third parties to hack into the user account easier. The information obtained through these websites can be used for identity theft to online and physical stalking and also blackmail.

A privacy controversy has arisen involving the most popular social networking site- Facebook. It was alleged that user pages were viewed by Facebook even though the user was not logged in and the user IP address was sent to the Facebook server. Facebook claimed that they used cookies for security purposes only and the cookies placed on the user's computer automatically downloaded WebPages even after the user has logged out. Facebook further claimed that software automatically downloaded the information and sent it to the social networking servers. Facebook has settled the claim and according to them, cookies sent information only when the user logs in and not otherwise. Therefore every user should delete cookies after login to secure their WebPages.

Orkut, also a popular networking site, faced criticism when the school student, a son of rich businessman was tracked through and murdered. A false profile of victim was apparently made,. Several days before boy's death his profile was tampered and all the pictures, videos were deleted and the profile was active even after victim's death.

Social networking sites offer varying level of privacy settings while encouraging users to give out personal information on the website. However various privacy activists worldwide are increasing pressure to build effective security systems to enable exchange of messages and information without violating privacy rights.

The big wave of social networking sites [5]

The big wave of social networking sites has hit almost every corner of the world in cyberspace. The huge popularity of the social networking sites has caught us by surprise. It was recently reported by Facebook and the University of Milan that the number of acquaintances separating any two people in the world was not six but 4.74. In India, 84 per cent users visit social networking sites which makes India the world's seventh largest social network's site visitor. Founded on 4 February, 2004 by Mark Zuckerberg, CEO and founder of Facebook, the website is a social utility site that enables people to remain connected with each other through sharing views on "wall" and instant messaging and sharing of photographs or videos. Facebook currently has more than 350 million active users across the globe. Twitter, another popular social networking platform is an information network that enables a person to join a group of his interest and become a 'follower' and receive updates whenever a member of the group posts a message known as 'tweet' on twitter. Twitter has more than 75 million user accounts. According to recent data available on the internet, Facebook membership has grown from 664 million users in first quarter of 2011 to 835.6 million in first quarter of 2012.

The introduction of the Unique Identification Regime in India has gone a step further in using technology to create and declare the identity of every Indian in cyberspace. An Indian will be recognized through biometrical retina scanning and given an identity number. That is the power of Information Technology! The domain of Information Technology and wonders it can achieve are only expanding day-after-day. We recently learnt that eye lenses with a microchip installation within will soon be invented that can store and read e-mail or other electronic data wirelessly! It will not be surprising that from a palmtop, a computer can function through a microchip in an eye lens smaller than the size of a peanut! Scientists have created a robot that can use Smartphone as its brain. One only

[4] Vishwanathan, Aparna In cyber law India and international perspective on key topic including data security, E commerce, cloud computing and cyber crimes, LexisNexis, 2012 Page 238

[5] Seth, karnika, Computer Internet and new technology laws, updated edn. 2013,, LexisNexis page 504

needs to put a wheeled chassis on a smart phone or ipod touch that enables one to use the device as the human brain. The controls for the device are embedded within the phone and can be downloaded as applications.

Impact of social networking sites

These platforms have a positive socio-cultural impact as it allows people to share their views with their distant friends and relatives within few seconds. It has negated the effects of geographical distances in our social lives. Culturally, it extends an enriching experience as one can make friends on these sites and learn about important events and festivals and life styles of different countries within one virtux room and share this experience with a group of friends. We can leave a message for a friend immediately on a telephone even though we may be apart by long physical distances. It will not be wrong if we admit we have cloned ourselves through technology and lead dual existence—one in the virtual world akin to an avatar and one in our physical surroundings—the tangible self that is bridged through communication devices such as laptop and cell phones.

Technology also works as a powerful tool to disseminate knowledge and information as more number of readers join e-libraries, subscribe to online journals, buy e-books or read newspapers. The economic impact is also positive as it is highly cost effective and time saving and also creates new opportunities for people to learn about new projects and deals. Internet is a powerful medium to exercise one's right to freedom of speech and expression, a fundamental right protected by Article 19 under the Constitution of India. But there is a flipside too. Many people fail to understand when free speech can be regarded as hate speech, defamatory, offensive, menacing, insulting, annoying, politically or religiously sensitive, against public morality or decency or likely to create public disharmony. People also do not understand the implications of creating a fake profile, messaging offensive materials, impersonating or posting some one's pictures or contact details without that person's permission. All these are violations of law and different provisions of the IT Act, 2000 read with Indian Penal Code, 1860 apply and prescribe punishments for committing these acts. These legislations place reasonable restrictions on our right to freedom of speech which the Constitution of India allows under Article 19(2) on grounds of protecting interests of the sovereignty, integrity of India, the security of the State, -friendly relations with foreign States, public order, decency or morality or in connection with contempt of court, defamation or incitement to an offence.

Offences attracted by publishing illegal content on social networking sites [6]

Section 66A of IT Act, 2000 expressly prohibits sending of any message through computer, or communication devices such as cell phones, that are grossly offensive or of menacing character, (that is disturbing in nature and unpleasant), any false information that causes annoyance, inconvenience, danger, or obstruction or is defamatory, injurious or insulting, or criminally intimidating or threatening. It also prohibits such false messages which are likely to spread enmity, hatred, or ill will or impersonating mails which are known as spoofed messages. Such acts are punishable with imprisonment for a term which may extend to three years and fine, it is a cognizable but bailable offence under IT Act, 2000. In addition, if a person fraudulently misuses any other person's password or unique identification feature, such act is punishable with up to 3 years punishment and fine up to one lakh.9, Punishment for cheating by personating is provided by Section 66D of the IT Act, when someone uses any communication device such as a cell phone or a computer to cheat by personating as another person. In one such case, a jilted lover created a fake profile of his ex-girlfriend and was arrested by law enforcement officials and investigations in the case are underway. These sections are frequently invoked in cases involving creation of false profile on Facebook or other social networking sites coupled with other sections of Indian Penal code, 1860 such as "Section 500 where defamation is also involved and an imposter writes derogatory comments about the person he is impersonating. In another case school student create fake profile of the Chief Minister, Shivraj Singh Chouhan on Facebook and placed cartoons and controversial materials on it from a cyber café was arrested by Indore Police. In a case a person on his Facebook profile publishes content that he was secured after making unauthorized intrusion into a computer system protected for national defense and knowing it likely to cause injury to India's sovereignty, integrity or security of State or friendly relations with another State, or will outrage public order, decency, and morality. (Including by hurting religious or political sentiments of people causing riots), and writes defamatory content, such act will be considered as cyber terrorism under Section 66F of the IT Act, 2000 which attracts punishment of imprisonment that can extend up to life imprisonment. Similarly, in case a person tweets an obscene message on twitter, he can be held liable for such act under Section 67 of the IT Act, 2000. In one defamation case Cairn sued Modi for sending tweets alleging he was a match fixer and UK courts granted approval to Cairn to pursue legal action for libel." The court held that Cairn resided in UK and is directly affected by number of people who received tweets in London and even if it is a single receiver, number of people that receive a libelous message is only one of the considerations in defamation actions. In another case, two men were imprisoned for writing defamatory remarks about Sonia Gandhi on Orkut, a social networking site. Recently, an Indian court dealt with a case challenging legality of opening minor accounts on Facebook. The Delhi High Court issued notice to the Union Government to explain how it was allowing minors to set up accounts on Facebook and Google.

Censorship of third party on social networking sites [7]

Recently, the issue of pre-censoring the third party information posted on social networking sites like Facebook and twitter came into limelight. The Hon'ble Minister for Information Technology, Mr. Kapil Sibal, had urged social networking sites to monitor the third party content they published on their sites as defamatory content existed on social networking sites which was damaging as the reach of Internet is pervasive beyond borders. The extant IT laws in India requited such sites to take off such illegal content within 36 hours from actual notice of knowledge of content if they do

[6] Ibid Page 504

[7] Ibid page 506

not monitor or edit content posted by third parties. Social networking sites contended that due to magnitude of content posted on daily basis such filters and pre-censoring was not possible on technical and administrative standpoint. While most sites use filters to check pornographic posts, to my mind there are technical problems in managing vocabulary of terms to sift out legal from illegal content. As it brings within its ambit fairly broad category of offences such as any content that is menacing or offensive, harmful to minors, insulting may fall in its ambit as "preventing incitement to commission of a cognizable offence relating to public order is one of the grounds that allows blocking under section 69 A of IT Act. 2000. One of the cognizable offences under I T Act 2000 is sending messages using a communication service as per section 66A of IT Act, 2000. The meaning and ambit of offensive messages or menacing is also unclear and may involve subjective interpretation as it is not defined by the IT Act, 2000. Meaning of "defamation" may also vary from jurisdiction to jurisdiction. Further Rule 3(2) of the 1T (Intermediaries Guidelines) Rules 2011 mandates removal of an illegal content posted by a user within 36 bonus of complaint by an aggrieved person on various grounds that are not objectively by the IT Act, 2000 or rules and may be misused to breach privacy and free speech on internet. In particular, the terms such as 'grossly harmful', 'harassing', 'blasphemous', 'hateful', 'ethnically objectionable', 'harmful to minors,' are subject to different subjective interpretations. In certain situations such content as described by Rule 3 of IT (Intermediaries Guidelines) Rules, 2011. when complained of by an aggrieved person may fall outside purview of Section 69A of IT Act, 2000 as it may not have any element or the required degree of seriousness to satisfy ' public order' involved although it may have element of 'incitement to commission of a cognizable offence' under Section 69A. Also, if government proposes to pre-censor such third party content, then clear rules that define ambit and scope of such regulation, including due diligence process for filtering by intermediaries ought to he passed and its technical and administrative feasibility also should he considered. The scope and ambit of terms "harmful to minors", "harassing" "hateful" found in Rule 3 of IT (Intermediaries Guidelines) Rules, 2011 may be clarified with the help of illustrations as found in the Indian Penal Code, 1860, For example, on consumer blogs complaining about deficient services of a service provider is protected by free speech so long, as it does not use abusive language or becomes defamatory. Therefore, netiquette needs to evolve in cyberspace so that users are aware and are able to distinguish form of free speech that is protected and content that becomes illegal.

Protecting privacy on social networking sites [8]

Another aspect to be considered in context of social networking sites is the protection of privacy. Because so much personal information is shared through such platforms, it is important to accept some one as a member of your group only it one is well acquainted with that person. In fact in China, Government has made it mandatory for all persons to use their true names instead of anonymous names on social networks due to difficulties faced by law enforcement agencies in tracking cyber criminals. Facebook and other networks require users to register their mobile numbers apart from name and e-mail address for registration and activation of user accounts. Therefore, a lot of personal information is shared with an intermediary like social networks that ought to keep such information safe as per Section 43A of the IT Act, 2000. Diminishing privacy standards and lack of netiquette on social networks has even been a cause of murder as witnessed in case of Adman, son of a businessman whose profile on Orkut reflected that he had gone to meet an impersonator called Angel when he. Was allegedly murdered by his own group of friends. Posting anyone's sensitive information about credit card numbers, internet pin, and any other sensitive information is an offence and one can suffer civil as well as criminal liability for such acts making the person liable to pay damages or compensation as well as face imprisonment or fine if such acts were intentional or done with due knowledge that it were illegal.

Unfolding benefits of social networking sites [9]

A positive feature of social networking sites is that these portals are proving useful to law enforcement authorities. As a protection against cyber-bullying, in 2011 Thames Valley police officers were reported to have used Facebook to identify and take action against cyber- bullies. With assistance of volunteers, the police investigated Facebook pages when it received complaints of cyber-bullying. A Facebook message was sent to offender to warn the offender and the student's parents are also informed of the incident and the warning letter.

As a positive step in India different government department are logging into social networking sites to accept complaints and provide free redressal against offender, of traffic violations or railway passengers such as the Delhi traffic Police.

Comments posted on such sites are being used as secondary evidence in legal proceedings produced before a court of law. Under Indian Evidence Act, 1872 although presumption of authenticity lies in favour of an electronically signed message under Section 85A and 85B of Indian Evidence Act, 1872 comments which are not electronically signed can also be produced as secondary evidence. Section 63 defines secondary evidence and includes copies made from original processes which in themselves ensure the accuracy of the copy. and copies compared with such copies. In case an e-mail or comment on social networking site is produced as evidence, it can be produced as secondary evidence as according to section 65-d, secondary evidence is allowed when original is of such nature that is not easily movable. In fact social networking sites are 'intermediaries' under IT Act, 2000 and may disclose information to law enforcement agencies when requested as per Rule 67(c) of the IT Act, 2000 and Rule 3(7) of IT (Intermediaries Guidelines) Rules, 2011. This evidence is used in divorce cases or cyber buying cases on social networking sites.

Suggestions on nettiquette on social networking sites

Thus, while using social networking sites it is prudent to adopt best practices to safeguard one's privacy and prevent any violation of law. It is advisable not to invite people you do not know to join your group, limit posting your or someone else

[8] Ibid Page 507

[9] Ibid Page 512

personal sensitive information or any infringing or harmful materials on social networking site, not to disclose for example, no one is at your residence on particular day during chatting as unlawful interceptions are possible by cyber Criminals. Also while posting any comments avoid posting any hate speech or use of abusive language and avoid writing such comments that are likely to ht considered obscene or that may create public disharmony or hurt religious sentiments of others. Simply voicing a consumer's concern or view on a topic acceptable as long as it is not accompanied by hate speech or abusive language is not defamatory, that is, avoid making deliberate false imputations that art derogatory to an individual or entity.

Bloging

What is blog?

A blog is a mix of the two words web and logs. It is a website or a section within a website maintained by an individual called the Administrator who regularly update his comments on a particular subject and invite comments from others who also post their responses on the blog. If content is filled by mobile it is termed as mob log (for example, twitter that can be accessed *via* mobile too) or if it contains videos it is a vblog. Example of a vblog is youtube website. It often contains textual matter mixed with images, videos, audio clip and other forms of multimedia. Twitter is also an example of `micro blog' with restriction of 140 characters or less characters that are transmitted and shared with groups on twitter network. Some blogs are static and do not have the feature of posting comments of users on the blog. However, interactive blogs are most common and blogging has become one of the most common means or self-expression. A blog is different from a Wiki as Wiki is a collaborative website that allows different users to write and update an encyclopedia on a topic or interlinked subject matter. Initially blogs were pages where individuals would pen down their personal diaries, and slowly it became a powerful tool to discuss social. Political and religious issues. Israel was amongst the first National governments to launch official blog for Israel. We also come across blogs which are directed at advertising, some publish information about an organization and its activities. Others could be entertainment blogs that discuss travel and lifestyle or music and theater. The popularity of blogging has dynamically increased in the past few years. According to a latest data available on the internet, bloggers increased from 3 million in July, 2004 to 164 million in July, 2011 in the world. These data projects that approximately 49 per cent bloggers belong to USA, 12 per cent in Asia pacific 29 per cent in Europe and 7 per cent in Canada and Mexico and 3 per cent bloggers live in South America. Among them most popular topics on blogs personal musings, (18 per cent), internet and technology (14 per cent), science (2 per cent). News (2 per cent), travel (3 per cent), family (2 per cent), and politics (8 per cent). Business (5 per cent), health (2 per cent) and 3 per cent others [10].

Role of social media in e-governance [11]

Realizing the vast potential of social media through social networks, blogs, and other forms of social networks such as professional network site 'linked in', the Indian Government has made several e-governance initiatives such as National Capacity Building Framework that aims to build capabilities of "Panchayats" and Citizen's Report Card Initiative· That collects and assesses citizen's feedback on government managed services, Nagrik Sahyog Kendra or Citizen Cells. Social media is becoming popular and various government agencies are using the medium for law enforcement initiatives. Delhi Traffic police joined Facebook and twitter to deal with traffic related issues. The Indore police is using twitter, blogs, online and mobile complaint process, goggle map of police stations and electronic crime mapper to track cyber-crimes. Maharashtra Police introduced SMS-based complaint tracking system called "Turant Chovis" for complaint response within 24 hours and redress within 30 days. The public diplomacy division of Ministry of External Affairs adopted social media through twitter with user id "Indian diplomacy" to connect with general public on current issues of concern." Also, the Municipal Corporation of Delhi launched a forum on Facebook to interact with citizens." Recently, the Indian Government has proposed institutionalizing citizen engagement in every e-governance project and drafted a 'Framework and guidelines for use of Citizen Engagement and Social Media by Government organizations', which as on date of writing is under discussion. Also, a basic framework and guidelines for use of social media by government agencies in India has been formulated. These guidelines assist agencies to create and implement their respective strategy for using social media, in particular to understand objectives, platforms, resources for interacting with citizens. These guidelines apply to all governance projects implemented at Central or State level. Likewise, in United States government has created a White House Facebook page, and a new social network site govloop.com within US department of Homeland Security to share its own experiences in policy making with other government departments and citizens. In Australia a government 2.0 taskforce is working on open government using social media to create transparency in government's functioning.

Bloging and Free speech

On one hand, blogging is considered as medium of expressing thoughts freely, on the, other hand, it can mean abuse of journalism. This is because it is a powerful medium to spread one's views but if the content is false or malicious, it is likely to mislead the public. This makes bloggers liable for defamation. In 2009, NDTV issued a legal notice to Indian blogger named Kunte for creating a blog post that criticised NDTV' coverage of the terrorist attacks in Mumbai. Subsequently, the blogger withdrew his post and gave a legal undertaking that his post was defamatory and, contained false information. Similarly another Indian blogger, Pradyuman Maheshwari decided to close his blog Mediaah Weblog when on criticizing the Times of India in his blog, he was served a

[10] http://www.invespcro.com/blog/how-big-is-blogsphere/ accessed on 30/03/2016

[11] Seth, karnika, Computer Internet and new technology laws, updated edn. 2013,, LexisNexis page 518

legal notice alleging offence of defamation. In a recent case instituted by a model named Liskula Cohen whose photograph was on the cover of Vogue Cohen was defamed as "shankiest in NYC" on a blog. The Court ordered Google to disclose the identity of the anonymous person who had posted the comment.

Liability of intermediaries on blogs

In most cases, the internet service providers are not liable for third party content that is posted by a blogger on its site unless it monitors and edits its contents which will attribute fulfilment of actual knowledge. This position applies in India as well as United States. On 9' May, 2012, in *Vyakti Vikas Kendra v Jitender Bagga* [12],'' Delhi High Court dealt with a case where, in a suit for injunction and damages, an interim injunction was ordered against defendants restraining publication of highly defamatory materials about His Holiness Sri Sri Ravi Shankar, owner of Art of Living Foundation, on www_blogger.com, in a blog that was created by defendant no.l. Plaintiff No. 1, Vvakti Vikas Kendra, India Public Charitable Trust, is a registered Public Charitable Trust constituted to implement and promote the spiritual, educational, social and developmental activities for The Art of Living in India that sought the restraint orders and other plaintiffs were followers of the Art of living. The court observed that Defendant No. 2 is an intermediary within the definition of Section 2(1)(w) and Section 79 of the Information Technology Act, 2000. Under Section 79(3) (b) of the IT Act, 2000, defendant No. 2 is under an obligation to remove unlawful content if it receives actual notice from the affected party of any illegal content being circulated/published through its service. The court further observed that Defendant no. 2 is bound to comply with Information Technology (Intermediaries Guidelines) Rules 2011. Rule 3(3) of the said rules read with Rule 3(2) requires an intermediary to observe due diligence or publish any information that is grossly harmful, defamatory', libellous, disparaging or otherwise unlawful. Further**,** the court noted that Rule 3(4) of the said rule provides obligation of an intermediary to remove such defamatory content within 36 hours. On the basis of said facts, the court directed that the defendant no.2 to remove all defamatory contents about the plaintiff posted by the defendant no.1 was also restrained from sending any e-mail including e-mails, or posting any material over the Internet which has a direct or indirect reference to the plaintiffs or The Art of Living Foundation, or his Holiness Sri Sri Ravi Shankar. Hence as per Indian laws, if on actual notice from affected party, the blog is not removed, the intermediary is liable for third party content that is unlawful. The internet service providers in United States may be liable for defamation 'copyright infringement or child pornography if they transmit and circulate such objectionable content with due knowledge or monitoring control. In the Communications Decency Act, 1996, section 230(c) (I) limits liability of Network Services Providers. In *Zeran v Americo,' Online Inc* [13], the Court observed that Section 230 aims to encourage self-regulation and provide immunity to internet service providers as against third party content posted by users. In *Playboy Freno* [14], the district court held the operator or bulletin board (a predecessor of a blog) on which a third party posted images of Playboy infringed distribution rights of Playboy. It further held that intent to infringe is not required in copyright infringement. In another bulletin hoard *case, Stratton Oakmont, Inc v Prodigy Serv's Co* [15]. the plaintiff a securities investment firm initiated a legal action against Prodigy Services Company for defamatory posts made by an unknown person against the plaintiff. The court took the view that Prodigy's role was more of an original publisher than a distributor because it advertised that it had control over the content that was published and in practice it regularly filtered and edited content on its bulletin board using special software." Later in *Lumley v ProdigY Services Company* [16],*"* an imposter posted messages in plaintiff's name on a Bulletin board system and sent defamatory mails to a third party. In the action for defamation and negligence, the court looks the view that Prodigy was only a conduit: as regards e-mail message and had no control over content being e-mailed: As regards BBS, the court held Prodigy has reserved a right to screen its bulk"! Board but it does not change its passive nature in *"millions of other messages in whose transmissions it did not participate"*. Hence, court did not agree t*hat* Prodigy was a publisher, which order the Court of Appeal also later affirmed.

Avoiding IP Infringement on blogs

A direct legal implication of improper blogging is when bloggers do not maintain originality of content and may engage in copyright infringements by uplifting and publishing content from other websites. This constitutes an offence of copyright infringement under Section 6 of the Copyright Act, 1957 which is punishable with imprisonment of not less than 3 months and may extend to 3 years and fine of not less than INR 50,000 which may extend to two lacs. Also, a blogger who manages a blog must mention in its terms of use that comments posted on blog by a user are shall he deemed to be copyright licensed and will be considered royalty free. Images which are copyright of others should not be posted on a blog otherwise it will: amount to a copyright infringement. Also surface linking is acceptable with prior permission but deep linking into another website or blog is generally considered unacceptable as netiquette and may involve copyright violations. Sometimes it may also be related to trade mark or framing and infringement of one's confidential information, trade secrets or proprietary rights.

Lacunae under it act (intermediary's guidelines) rules, 2011

While these rules clarify role and liability of ISPs, it has several lacunae that deserve immediate correctional measures. Rule 3(4) of the said rules states that where an intermediary (including blog service provider) on its own or on actual knowledge receives a complaint from an affected party in writing duly signed by electronic signature complaining of the unlawful content, it is responsible for disabling such content within thirty six hours. Application of these provisions is likely to curtail freedom of speech and expression on the internet. Also, because the ambit of its application is quite

[12] 2012 AIR (Del)180
[13] 524 US 937 (1998)
[14] 839 F Supp1552 (M.D.Fla11993.)
[15] 1995WL 323710
[16] 94 N.Y. 2d 242

large and vague, any form of objection or criticism may fall foul of the provision. Unless the intermediary verifies identity of person aggrieved, and checks if there is a legitimate complaint based on a legal provisions, every frivolous complaint will be entertained by ISP leading to over censorship and removal of even legally valid content from internet. For example, those portals that display public opinion or consumer dissatisfaction may also fall within banned categories of Rule 3. For this reason it is important to provide illustrations to define scope of application of legal terms such as "harmful to minors", "harassing", "offensive", "menacing", to prevent subjective interpretation and impart objectivity. Otherwise, this may amount to censorship on internet beyond what is reasonable. Therefore, it is advisable to illustrate that writing consumer reviews is protected by free speech so long as it is not defamatory or uses abusive language to voice consumer dissatisfaction. The intermediaries are required to preserve the information for at least ninety days for investigation. This period is in fact inadequate to conduct any meaningful and effective investigations of cybercrimes and should be reconsidered by the Central Government. The Rule 3(11) requires intermediaries to publish name of grievance officer and establishment of a redress mechanism for complaints by users against other persons who act in violation of Rule 3. Such complaints are required to be resolved within one month from the date of receipt. Effectiveness of the grievanc[e] redressal system will depend on checks and supervision that may be exercised on intermediaries to resolve consumer disputes within stipulated time frame Without such supervision, success of such schemes does not seem realist[`'] Also, unless grievance redressal officer is legally qualified, he may be Liable differentiate legally valid complaints from frivolous complaints. This renders the provisions vulnerable to misuse and abuse.

Further, Rule 3(5) obligates an intermediary to inform the users of its rights to terminate forthwith any services offered to users in case of breach of any term of privacy policy or user agreement. Therefore if blogger breaches any term of use, he can be debarred from posting any comments on a blog. In addition Rule 3(7) requires an intermediary to provide information and assistance to government agencies for investigation and cyber security reasons. Such assistance is required from intermediary for verifying a person's identity. For prevention, investigation, detection, cyber security incidents and punishment of offences. Here the rules fail to address the issues I' anonymous blogging. The rules do not stipulate that those websites that allow anonymous blogging must store some identification mechanisms such as IP addresses so that if questioned by a government authority their actual identities can he disclosed for investigation purposes. Hence all blogging sites that facilitate blogging and posting of third party content to the best practices as well as the rules framed for intermediaries described hereinabove. It is pertinent that existing lacunae in rules dealing with intermediary guidelines are clarified and supplemented with additional laws to address the existing lacuna and ambiguities in the Indian legal framework. It is also advisable that Bloggers and bloc, administrators Observe terms of use and use the suggested best practices in order to avoid violation of any law and yet convey their viewpoint on a subject matter effectively through bloggingg.

Conclusion

Keeping in mind the convergence and rapid development in communication technology few very good steps has been taken such as communication device and intermediary has been defined. A new section has been inserted namely section 10A and via this section validity of e-contract has been reinforced. Another good is inserted through section 46(5) and according to this section executing powers of Adjudicating officer is at par with civil court. A number of new provisions have been inserted under chapter XII in order to combat with various kinds of cyber-crimes which have taken their roots recently such as child pornography, and cyber terrorism. Intermediaries have been placed with extra burden to provide access to enforcement agencies to sensitive information so that enforcement agencies may be able to solve certain cyber-crimes such as cases under section 67C, section 69 etc. One of the important provisions which has been inserted is that liability of Internet Service Providers has been revisited and now it shall be responsibility of the complainant that ISP was lacking in due diligence or there was presence of knowledge on the part of ISP, now proving conspiracy on the part of ISP will be difficult. These are few challenges which will be hurdle in the way of enforcement agencies while intercepting traffic data and communication over Internet as the amended provisions require strict compliance of rules and regulations. Power of blocking has also not been so easy now and it should be exercise carefully so that it should not amount to unreasonable censorship. One of the biggest lacunas that it has is that although many of the offences have been made cognizable but bat the same time they have also been made bailable. In this situation there is likelihood of tampering evidence by cyber-criminal once he is released on bail. There are certain other shortcomings which have not been discussed properly, these are following: Spam is identified as Unsolicited Bulk E- mail. In the beginning bit was not taken seriously but after some time it was felt that it is creating economic hurdles. Presently it is unregulated as there is neither technical protection nor legislative protection which is serious issue. In IT Law spam has got no place at all while in US and European Union they have legislation regarding spam and in this sequence Australia has toughest law which fines up to 1.1 million per day in case of violation. Phishing is also one of the major problem from which IT industry is suffering. Phishing means attempting to acquire sensitive personal information fraudulently such as usernames, passwords, credit card details etc. Presently there is no provision regarding Phishing in IT Law, however IPC talks about cheating but IPC alone is not able to regulate the activity of phishing which is too broad to handle for IPC.

References

1. Dianne Timm M, carolyn J. duven, privacy and social networking sites 24, wiley interscience. 2008.
2. Social Networking Privacy: How to be Safe, Secure and Social available at https://www.privacyrights.org/social-networking-privacy-how-be-safe-secure-and-social accessed on 28/03/2016
3. Cyber-stalking: the Regulation of Harassment on the Internet By Louise Ellison and Yaman Akdeniz available at http://www.demonish.com/cracker/1431329602_58a7349092/stalking_article.pdf. accessed on 29/03/2016

4. Vishwanathan, Aparna In cyber law India and international perspective on key topic including data security, E commerce, cloud computing and cyber-crimes, Lexis Nexis. 2012, 238.
5. Seth, Karnika. Computer Internet and new technology laws, updated edn., Lexis Nexis. 2013, 504.
6. Ibid Page 504
7. Ibid page 506
8. Ibid Page 507
9. Ibid Page 512
10. http://www.invespcro.com/blog/how-big-is-blogsphere/ accessed on 30/03/2016
11. Seth, Karnika. Computer Internet and new technology laws, updated edn., Lexis Nexis. 2013, 518.
12. 2012 AIR (Del)180
13. 524 US 937 (1998)
14. 839 F Supp1552 (M.D.Fla11993.)
15. 1995WL 323710
16. 94 N.Y. 2d 242