LAW MANTRA THINK BEYOND OTHERS
(I.S.S.N 2321- 6417 (Online)
Ph: +918255090897 Website: journal.lawmantra.co.in
E-mail: info@lawmantra.co.in contact@lawmantra.co.in

Right to Privacy in the Social Networking Era*

INTRODUCTION

In today's social world, most of us find that our lives have become considerably dependent on the internet and are intensely connected with a number of social networking sites. The users, without giving it a second thought, tend to share almost every tidbits of their personal information online. It has, thus, become possible for anyone having preliminary knowledge of the working mechanism of the World Wide Web to acquire, as a minimum, some of the personal information about anyone on the same platform one wishes to be friends with, marry, employ, investigate or for that matter, even stalk.[1] Today, most of the people are increasingly using the social networks, like MySpace, Facebook, Orkut, Twitter, Linkedin, etc. These online platforms let users share or publish details about themselves, their emotions and their lives. Further, they also provide space to its users in order to remain connected with their friends, relatives and colleagues. Nonetheless, there exists some information which is expected by the user to remain private and unpublished so as to protect it from third party intrusion, is in reality revealed online. In the case of countries like India, social media users barely think about the likely consequences before revealing their personal information. Even a little piece of information becomes capable of being promptly located and harvested by those individuals who can easily get hold of social networking sites.

The following line holds significance in the present context: "If you feel like someone is watching you, you're right. If you're not doing anything about this anxiety, you're just like almost everyone else."[2] Such unmindfulness of the users and its serious repercussions have aroused a strident outcry of protest led by advocates of privacy who have contended that the free flow of information on the internet has, actually, made us less free.[3]

Thus in the light of the above stated information and recent developments, various illustrations would be discussed wherein the privacy of a user has been comprised. Further, the existed legal remedies to check such infringements would also be analyzed in the succeeding parts of the paper.

2. THE RIGHT TO PRIVACY- A CONCERN

"You Have Zero Privacy Anyway. Get Over It"

- Scott McNealy, CEO of Sun Microsystems

There have been two facets of almost everything mankind has ever come up with and internet is one of them. As per the research of a leader in measuring the digital world, ComScore, as many as 84 percent of the total users of internet in India are registered on various social networking sites.

*Ms. Neha Sharma, III Year, B.A. LL.B. (Hons.), Rajiv Gandhi National University of Law, Punjab

[1] Corey Ciocchetti, *Just Click and Submit: The Collection, Dissemination and Tagging of Personally Identifying Information*, 10 VAND. J. ENT. & TECH. L. 553, 556 (2007-08).

[2] Bob Sullivan, 2011.

[3] Daniel J. Solove, The Future of Reputation Gossip Rumour and Privacy on the Internet 2 (2007).

LinkedIn, the world's largest online professional network with over 364 million members globally, said it has crossed 30 million members in India making it the largest market for LinkedIn after the US in terms of member base.[4] Technological advancement has dominated the working of our lives. We cannot be certain in such an era if our personal information and communication has been privately known by a third party or not, a situation might occur of 'wherever you go, our network follows'. It will, therefore, not be wrong to say that there is only a narrow line between private and public life of an individual in the age of social networking. Once image, personal data or video has been shared on the concerned website, one becomes helpless to exercise control over its distribution. Even if the privacy settings have been well put off, there exists an unknown web administrator to whom unknowingly data is being shared.

The international media had described the sudden increase in the number of Facebook users over the past decade in very subtle yet interesting ways: Facebook, it proclaimed, had become the world's third largest nation in terms of the size of its population.[5] This meteoric rise was, nonetheless, followed by the uncovering of a story of a security consultant who, by using a fairly sophisticated code, scanned Facebook profiles in order to collect data that had not been hidden by the users as per their privacy settings.[6] Another story hailed from MIT wherein a group of students developed such a Facebook application which was capable of examining the entire profile of a user and determining if the user was heterosexual or not.[7] Such news reports of privacy abuse are only a few instances of a larger course, further they also highlight the underlying fact that the personal information of a user has a fundamental importance and thus, its misuse poses actual and substantial risks to the privacy of a user.

The unparalleled intensity of sharing information that occurs on social networking sites on a daily basis has severe implications on the privacy. The efficacy of the settings relating to the privacy controls of Facebook has been now frequently challenged. The common practice within such social networking sites is to set a prejudiced privacy setting as default so that anyone can see the information shared by an individual unless he actively changes them. As a consequence of this, a substantial number of the users unconsciously allow free public access to the information personally identifying them, merely because of failure on their part to change the default privacy settings.[8] This criticism was also justified by a research study which concluded that around 44 percent of adult Facebook users and 41 percent of children Facebook users have open privacy settings.[9] Several critics have considered this as a flaw and underlying prejudice on the part of Facebook against sign up and privacy settings and the assumption that a user will want to share the maximum possible data.[10]

---

[4] "LinkedIn crosses 30-million member mark in India", The Hindu, Available at http://www.thehindu.com/business/Industry/linkedin-crosses-30million-member-mark-in-india/article7179938.ece (Last visited on August 30, 2015).

[5] "Facebook Population", The Economist, Available at http://www.economist.com/node/16660401 (Last visited on August 21, 2015).

[6] Daniel Emery, "Details of 100m Facebook Users Collected and Published", Available at http://www.bbc.co.uk/news/technology-10796584 (Last visited on August 21, 2015).

[7] Dan Macsai, "MIT's Facebook "Gaydar"- Is it Homophobic?", FastCompany, Available at http://www.fastcompany.com/blog/dan-macsai/popwise/mits-facebook-gaydar-it-homophobic (Last visited on August 22, 2015).

[8] Helen Anderson, *A Privacy Wake-Up Call for Social Networking Sites?*, 20(7) ENTERTAINMENT LAW REVIEW 245 (2009).

[9] Office of Communications, Government of UK, *A Quantitative and Qualitative Research Reports into Attitudes, Behaviours and Use*, Available at http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/socialnetworking/ (Last visited on August 22, 2015).

[10] "Dicing with Data", The Economist, Available at www.economist.com/node/16163396 (Last visited on August 22, 2015).

Nevertheless, only being able to change the default settings cannot be sufficient to protect the shared data so far as a substantial part of their personal data is held by someone else's Facebook page. Such as, a user may be tagged in a status, photograph or a comment posted by his friend; in this circumstance the user becomes incapable of exercising any control over posted data and the privacy settings applied by the concerned friend.[11] The launching of Google Buzz, Google's social networking feature, came up with similar problems. Google made it mandatory for the Buzz users to set up such public profile pages which contain a list of their contacts, by this means they automatically published a list of the most emailed contacts of the user.[12]

Due to the above-mentioned reasons, social networking sites such as Facebook have been called upon to do more in order to explain the intentions of stating such terms and conditions which are prejudiced to its users.

3. EXISTING LEGAL SOLUTIONS FOR PRIVACY INFRINGEMENT

3.1. Constitutional Provisions

The users of social media have contended, now and then, for a right to privacy which is not infringed arbitrarily by social networking sites. Many legal theorists and philosophers have, nonetheless, been fascinated by the concept of privacy.[13] The aim to give privacy a constitutional definition had remained evasive. The formulation of privacy as a 'right to be left alone'[14] has been criticized for being too broad and vague in nature. In the meantime, the understanding of privacy as 'limited access to self'[15] has attained legitimacy in some sections. The meaning attached to the term 'Privacy' as a right of restricted access to self implies that every individual has a right to decide the extent of public scrutiny and knowledge in her private life.[16] In the concerned context, privacy has also been construed as being a right to control over one's own personal information.[17]

The Supreme Court has recognized the right to privacy under Art. 21 of the Constitution by way of an expansive interpretation of the phrase 'personal liberty'.[18] This right, nonetheless, is not absolute.[19] The Apex Court has affirmed that as soon as the information of an individual falls within the public domain, the right to privacy in regards to that information ceases to exist.[20] A plausible opportunity can thus be carved out only from a logical construction of the term 'public domain'. The Court has also held that privacy is not violated if it is intruded by a fair, just and reasonable procedure, established under law.[21]

3.2. Tort Based Liability

One of the various categories of torts falling under the ambit of "invasion of privacy" is appropriation. Appropriation can be referred to the use of the name, likeness, or image of an

[11] *Id*.
[12] Nicholas Carlson, "Warning: Google Buzz Has a Huge Privacy Flaw", BUS. INSIDER: SILICON ALLEY INSIDER, Available at http://www.businessinsider.com/warning-google-buzz-has-a-huge-privacy-flaw-2010-2 (Last visited August 25, 2015).
[13] Daniel J. Solove, *Conceptualising Privacy*, 90 CALIFORNIA LAW REVIEW 1087 (2002).
[14] *R. Rajagopal* v. *State of Tamil Nadu*, (1994) 6 SCC 632.
[15] Solove, *supra* note 3.
[16] *Id*.
[17] *Id*.
[18] *Kharak Singh* v. *State of Uttar Pradesh*, AIR 1963 SC 1295; *People's Union for Civil Liberties* v. *Union of India*, (1997) 1 SCC 301; *Govind* v. *State of Madhya Pradesh*, (1975) 2 SCC 148; *District Registrar and Collector* v. *Canara Bank*, (2005) 1 SCC 496.
[19] *Mr. 'X'* v. *Hospital 'Z'*, (1998) 8 SCC 296.
[20] *Supra* note 14.
[21] *Supra* note 18.

individual for commercial interests without obtaining any prior consent of that individual.[22] The tort of appropriation has been recognized in various states, California being one example, of the United States. This tort tends at protect the privacy of an individual by ensuring protection to the individual's name or likeness.[23]

The tort of publication of private facts provides protection to an individual with respect to the publication of such facts which, even if true, will offend a reasonable person.[24] The concerned tort liability is, nevertheless, inappropriate, if the activities of the plaintiff have been observed in a public place or if such activities are considered worth reporting.[25]

With respect to breach of confidentiality it has been argued that at least some of the private information is bound to be breached in today's highly networked society. This tort grants that certain privacy breaches will certainly occur and, thus, this tort tends to focus on the duties owed within the chain of such a breach.[26] It has been suggested that the general rules of confidence will apply between the users of social networking *inter se*. This was proposed after the case of *Duchess of Argyll* v. *Duke of Argyll*,[27] wherein it was held that if a former girlfriend posts humiliating or intimate information about her boyfriend on Facebook for the world to know, she may fall well within the ambit of breach of confidence.

3.3. Contract Based Liability

The platform of social media provides for contractual terms and conditions at almost every place a person browses. Generally such conditions are unimportant; however, often these terms have a lot of significance attached to them. Such contractual provisions are usually in the form of privacy policies, community use guidelines or terms of use, *inter alia*, and these contracts may be executed by a traditional licensing agreement or services contract for use of the application or, commonly, through an online click-wrap agreement.[28]

The biggest setback to the enforceability of such privacy policies of social networking sites is the lack of free consent. A contract becomes enforceable only when both the parties to it have evidently given their full and free consent to all its terms and conditions.[29] The users are, however, bound only to those online agreements that mandatorily entail an obligation to view them in their entirety so as to complete an operation and click on - 'I Agree' (online click-wrap agreement).[30] The authorities of American jurisprudence suggest that simply calling for a user to click on a space to mark his intention of acceptance is not adequate if the user is not obligated to see the agreement for the request to be processed.[31] Thus, if users are took for consenting to any social networking site's privacy policy by account of being a member of that site, then the user can resort to argue that no enforceable contract was entered into by the parties as the mandatory requirement of fair consent was never given in true sense.

3.4. Data Protection

[22] Legal Information Institute, Available at https://www.law.cornell.edu/wex/appropriation (Last visited on August 24, 2015).
[23] J. Thomas McCarthy, *The Rights of Publicity and Privacy*, Available at http://west.thomson.com/productdetail/126362/13516725/productdetail.aspx (Last visited on August 27, 2015).
[24] Brian Kane, *Balancing Anonymity, Popularity and Micro-Celebrity: The Crossroads of Social Networking and Privacy*, 20 ALBANY JOURNAL OF SCIENCE AND TECHNOLOGY 327, 339 (2010).
[25] *Id*.
[26] Lawrence M. Friedman, *Name Robbers: Privacy, Blackmail, and Assorted Matters in Legal History*, 30 HOFSTRA L. REV. 1093, 1102 (2002).
[27] (1965) 2 WLR 790.
[28] Brett Lockwood, *Social Media Marketing: The 411 on Legal*, SGR LAW 28 (2010/2011), Available at http://www.sgrlaw.com/resources/trust_the_leaders/leaders_issues/ttl28/1597/ (Last visited on August 25, 2015).
[29] Indian Contract Act, 1872, Section 10.
[30] Mark A. Lemley, *Terms of Use*, 91 MINN. L. REV. 459 (2006).
[31] *Comb* v. *Paypal Inc.*, 218 F. 2d 1165.

India, unlike the European Union or the United States of America, does not have a comprehensive and all-compassing statute for the protection of data and digital privacy.[32] The provisions of the Information Technology Act, 2000 (IT Act) have been considered to be inadequate to deal with the privacy claims of the issues arising in the new technological era.[33] The first obstacle that has been incorporated in the Act is its narrow and restrictive definition of the term 'data' which necessitates it to be devised in a formalized manner.[34] The ambit of such conceptualization, however, remains hazy and does not provide protection to the data of users available informally on social networking sites.

An important provision in the Information Technology (Amendment) Act, 2008 (IT Amendment Act) is Section 43A which provides for the payment of compensation in case of a failure to protect any sensitive personal data by a body corporate.[35] The silence of the IT Amendment Act over any upper limit for the amount of compensation is applaudable, however, it is important to take note of the fact that in order to be eligible for any damages the plaintiff is supposed to prove that there was negligence on the part of the body corporate in preserving reasonable security practices. Furthermore, it is argued that the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal data or Information) Rules, 2011 made under Explanations (ii) and (iii) to Section 43-A render the concerned provision hollow and toothless.

4. SELF- REGULATION BY THE SOCIAL NETWORKING SITES

It is quite apparent that social networking sites have an innate inducement in securing the data of its users. A large user base not only facilitates recognition but also plays a central role in maximizing revenues as the volume of advertisements and licensed content is a direct function of the size of the audience to the website.[36] Simultaneously, it is essential for such sites to make an environment wherein involvement in the network is reckoned as a personal experience for users rather than disclosing the information to a commercial undertaking. In addition to that, the likely loss of status that may be caused to sites due to privacy infringements and the rationale for spur for self-regulation becomes evident.[37] The fact that social media users are no longer prepared to stake their privacy rights is clear from the widespread hue and cry that compelled Facebook to surrender on features such as Beacon and Google to introduce changes to Buzz. Another contention that is often put forth in favour of the case of self-regulation is the fact that the Parliament is a busy body, lacking the agencies to keep track of the innovations over the internet and ever developing methods of information sharing on social networking sites.[38]

The best example of self-regulation has been perhaps demonstrated by Google. Google, as a matter of its policy, anonymises all the information of the user that it collects making it impossible

---

[32] Madhavi Divan, *The Right to Privacy in the Age of Information and Communications*, (2002) 4 SCC (JOUR) 12.

[33] Vakul Sharma, "White Paper on Privacy", Available at http://iamai.in/Upload/IStandard/White%20Paper%20on%20Privacy.%202007.pdf (Last visited on August 28, 2015).

[34] Section 2: Data means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.

[35] Section 43-A: Compensation for failure to protect data.- Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

[36] Arun Mal & Jenisha Parikh, *Facebook & The Right To Privacy: Walking A Tight Rope*, 4 NUJS L. REV. 299 (2011)

[37] Anderson, *supra* note 8, 245.

[38] Robert Terenzi, *Friending Privacy: Toward Self-Regulation Of Second Generation Social Networks*, 20 FORDHAM INTELLECTUAL PROPERTY, MEDIA AND ENTERTAINMENT LAW JOURNAL 1049, 1099 (2010).

to trace the information to any particular individual user when such data is shared across application programming interfaces.[39] Subsequently, Google launched another program titled Privacy Dashboard which comprises of a meticulous list of all the applications of a user and allows her to set privacy preferences for each application separately.[40] As a consequence of these, Google seeks to gain the goodwill and thus win the faith of the internet users.

The above analysis leads the researcher to state that it is in the paramount interest of social networking sites to regulate themselves with a view to protect the privacy of a user. Nevertheless, there also exist unfavorable economic incentives and the likelihood of market failure. Therefore, despite the fact that there are limitations attached to the regulation of privacy standards by the government and judiciary, it is implausible to contend that they should step down from this field of regulation in its totality.

CONCLUSION

With the increase in use of social media the limits between work and play have been blurring. The idea of social media is primarily to provide a platform to the people where they can freely share feelings, information, pictures and data. Privacy, as discussed above, has often been construed as a matter of personal right of an individual to control the use of his data. However, a vast majority of social networking sites seem to have built a prejudicial structure around the user so as to extract his information and further misuse it or share it with the prospective advertisers and thus make money for themselves. It is thus evidently clear that the law needs to intervene in this matter so as to provide an open and safe cyberspace for the users. Unfortunately, nonetheless, the existing legal framework is very weak and inadequate so as to deal with such a right which is intrinsic to one's life. And, therefore, it can be concluded that the need of the hour is to bring in stringent laws and rules so as to shift the burden on the service providers to maintain a safe medium of social interaction for its users.

[39] Google, Google Privacy Center, Available at http://www.google.com/privacy.html (Last visited on August 27, 2015).

[40] Erick Schonfeld, "Google Gives You a Privacy Dashboard to Show Just How Much It Knows About You", Available at http://www.techcrunch.com/2009/11/05/google-gives-you-a-privacy-dashboard-to-show-just-how-much-it-knows-about-you (Last visited on August 28, 2015).