REVISITING THE CONCEPT OF PRIVACY VIS-À-VIS ADVENT OF SOCIAL MEDIA

Mr. Abhijit Rohi*

Introduction

Right to privacy has been recognized as a fundamental right as one of the facets of right to life and personal liberty (Article 21) under Constitution of India. The understanding of right to privacy still appears to be in its nascent stage in India as compared to the advanced legal systems like USA, UK and EU legal regime. With the change in the nature of media and the introduction of social media, right to privacy is at stake. For the better protection and realization of the fundamental right to privacy of every individual even in the cyberspace, the law has to take into account the different angles of right to privacy.

In this backdrop the paper tries to analyze the interface between social media and right to privacy. The question which the papers seeks to deliberate on is whether the present understanding of privacy, as is viewed from the existing legal framework, can conceptually be made applicable to the social media? If not, then, do we have to have a different take on the concept of privacy when it comes to regulating on-line privacy with special reference to social media. The issues relating to privacy such as recognition of right to secrecy, right to be forgotten, right to be let alone, and the concept of *privacy in public* are the focus of the deliberation in the light of the aforementioned question. The paper strongly advocates the need for revisiting our theoretical understanding of concept of privacy taking into account the nature of social media and the implications which it can have on the individual privacy.

The paper is divided into three parts. Part I deals with the understanding of right to privacy as per the interpretation given to mainly Articles 19 (1) (a), 19 (2) and 21, to carve out the said right. The pertinent judicial pronouncements have also been discussed to understand the conception of privacy in India. Also the existing legal regime protecting right to privacy in India is dealt with. Part II deals with the advent of social media and the threats it has posed for protecting right to privacy of individual on-line along with the advantages of it. Keeping in view the threats and the requirements to

* Assistant Professor, School of Law, Christ University, Bengaluru, India.

highlight the advantages the balancing is required to be done where the privacy is not affected and the advantages of the technology are available to the public. The balancing, the corresponding required understanding of privacy along with its different aspects as appeared in the existing legal framework are the focus of Part III followed by the conclusion advocating the need for the elaborate and comprehensive understating the right to privacy itself on theoretical level so as to be reflected in the requisite legal framework regulating privacy in India.

Part I: Right to Privacy: The Present Understanding in India

The five decisions by the Supreme Court in the succeeding 5 decades of Maneka Gandhi vs. Union of India[1] have established the Right to Privacy in India as flowing from Article 19 and 21. The first was a seven-Judge bench decision in *Kharak Singh v. The State of U.P.*[2] decided in 1964.[3] In a minority judgment in this case, Justice Subba Rao held that "the right to personal liberty takes in not only a right to be free from restrictions placed on his movements, but also free from encroachments on his private life. It is true our Constitution does not expressly declare a right to privacy as a fundamental right but the said right is an essential ingredient of personal liberty. Every democratic country sanctifies domestic life; it is expected to give him rest, physical happiness, peace of mind and security. In the last resort, a person's house, where he lives with his family, is his "castle" "it is his rampart against encroachment on his personal liberty." This case, especially Justice Subba Rao's observations, paved the way for later elaborations on the right to privacy using Article 21.

In 1972, the Supreme Court decided one of its first cases on the constitutionality of wiretapping. In *R.M. Malkani v. State Of Maharashtra*[4] the petitioner's voice had been recorded in the course of a telephonic conversation where he was attempting blackmail. He

---

1 (1978) 2 SCR 621.

2 (1964) 1 SCR 332.

3 The question for consideration in this case was whether "surveillance" under Chapter XX of the U.P.Police Regulations constituted an infringement of any of the fundamental rights guaranteed by Part III of the Constitution. Regulation 236(b) which permitted surveillance by "domiciliary visits at night" was held to be violative of Article 21.The meanings of the word "life" and the expression "personal liberty" in Article 21 were elaborately considered by this court in Kharak Singh`s case. Although the majority found that the Constitution contained no explicit guarantee of a "right to privacy", it read the right to personal liberty expansively to include a right to dignity. It held that "an unauthorised intrusion into a person's home and the disturbance caused to him thereby, is as it were the violation of a common law right of a man -an ultimate essential of ordered liberty, if not of the very concept of civilization".

4 AIR 1973 SC 157, 1973 SCR (2) 417.

asserted in his defence that his right to privacy under Article 21 had been violated. The Supreme Court declined his plea holding that "The telephonic conversation of an innocent citizen will be protected by Courts against wrongful or high handed' interference by tapping the conversation. The protection is not for the guilty citizen against the efforts of the police to vindicate the law and prevent corruption of public servants."[5] The third case in the series, *Govind v. State of Madhya Pradesh*[6] (1975), decided by a three Judge Bench of the Supreme Court, is regarded as being a setback to the right to privacy jurisprudence. Here, the court was evaluating the constitutional validity of Regulations 855 and 856 of the Madhya Pradesh Police Regulations which provided for police surveillance of habitual offenders which including domiciliary visits and picketing of the suspects. The Supreme Court desisted from striking down these invasive provisions holding that "It cannot be said that surveillance by domiciliary visit-, would always be an unreasonable restriction upon the right of privacy. It is only persons who are suspected to be habitual criminals and those who are determined to lead a criminal life that are subjected to surveillance." The court went on to make some observations on the right to privacy under the constitution: "Too broad a definition of privacy will raise serious questions about the propriety of judicial reliance on a right that is not explicit in the Constitution. The right to privacy will, therefore, necessarily, have to go through a process of case by case development. Hence, assuming that the right to personal liberty. The right to move freely throughout India and the freedom of speech create an independent fundamental right of privacy as an emanation from them it could not be absolute. It must be subject to restriction on the basis of compelling public interest."

This case is important since it marks the beginning of a trend in the higher judiciary to regard the right to privacy as "not being absolute". From Govind onwards, 'non-absoluteness' becomes the defining feature and the destiny of this right. This line of reasoning was continued in *Malak Singh v. State Of Punjab & Haryana*[7] (1980) where the Supreme Court held that surveillance was lawful and did not violate the right to personal liberty of a citizen as long as there was no 'illegal interference' and it was "unobstrusive and within bounds". Nearly fifteen years separate this case from the Supreme Court's next major elaboration of the right to privacy in *R. Rajagopal v. State of Tamil Nadu*[8] (1994). Here the court was involved a balancing of the

---

5 *Id.*
6 (1975) 2 SCC 148.
7 AIR 1981 SC 760.
8 (1994) 6 S.C.C. 632.

right of privacy of citizens against the right of the press to criticize and comment on acts and conduct of public officials.[9]

The final case that makes up the 'privacy quintet' in India was the case of *PUCL v. Union of India*[10](1997), a public interest litigation, in which the court was called upon to consider whether wiretapping was an unconstitutional infringement of a citizen's right to privacy.

On the concept of the 'right to privacy' in India, the Court made the following observations: The right privacy - by itself - has not been identified under the Constitution. As a concept it may be too broad and moralistic to define it judicially. Whether right to privacy can be claimed or has been infringed in a given case would depend on the facts of the said case."[11] This case made two important contributions to communications privacy jurisprudence in India – the first was its rejection of the contention that 'prior judicial scrutiny' should be mandated before any wiretapping could take place. Instead, the court accepted the contention that administrative safeguards would be

---

9 The case related to the publication by a newspaper of the autobiography of Auto Shankar who had been convicted and sentenced to death for committing six murders. In the autobiography, he had commented on his contact and relations with various high-ranking police officials – disclosures which would have been extremely sensational.
The right of privacy of citizens was dealt with by the Supreme Court in the following terms: - (1) The right to privacy is implicit in the right to life and liberty guaranteed to the citizens of this country by Article 21. It is a "right to be let alone". A citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, childbearing and education among other matters. None can publish anything concerning the above matters without his consent - whether truthful or otherwise and whether laudatory or critical. If he does so, he would be violating the right to privacy of the person concerned and would be liable in an action for damages. Position may, however, be different, if a person voluntarily thrusts himself into controversy or voluntarily invites or raises a controversy. (2) The rule aforesaid is subject to the exception, that any publication concerning the aforesaid aspects becomes unobjectionable if such publication is based upon public records including court records. This is for the reason that once a matter becomes a matter of public record, the right to privacy no longer subsists and it becomes a legitimate subject for comment by press and media among others. We are, however, of the opinion that in the interests of decency [Article 19(2)] an exception must be carved out to this rule, viz., a female who is the victim of a sexual assault, kidnap, abduction or a like offence should not further be subjected to the indignity of her name and the incident being publicised in press/media. On this reasoning, the court upheld that the newspaper's right to publish Shankar's autobiography, even without his consent or authorisation, to the extent that this story was able to be pieced together from public records. However, if they went beyond that, the court held, "they may be invading his right to privacy and will be liable for the consequences in accordance with 10 law." Importantly, the court held that "the remedy of the affected public officials/public figures, if any, is after the publication".

10 AIR 1997 SC 568.

11 *Id.*

sufficient. Secondly, the Court prescribed a list of procedural guidelines, the observance of which would save the wiretapping power from unconstitutionality.[12]

Though this being the case and understanding of the privacy as can be viewed in the form of the judicial pronouncements, the privacy of the individual in an on-line environment is equally important and so is to be protected.

Some other instances which have resulted in awareness about privacy in India in recent times (not necessarily to be online) are, in 2009, the Delhi High Court, in a major ruling, 'read down' Section 377 of the Indian Penal Code which had been previously used to criminalize homosexuality in India. A major plank of the ruling was an affirmation of the citizen's right to privacy which the court upheld as fundamental. This case was also brought to the Delhi High Court as a PIL by an NGO called the Naz Foundation.[13] In February 2010, in a much publicized case, a senior professor of Aligarh Muslim University – one of the oldest in the country – was suspended after students "set up cameras to catch him having consensual sex with a rickshaw-puller in his campus home".[14] Many universities and schools in India have installed extensive CCTV camera networks on their premises. In January 2011, the Maharashtra Government passed a resolution requiring all universities in the state to install a biometric card system on their campus.[15] In February 2011, fingerprint data was captured from over 11,000 aspirants writing an entrance exam for Post Graduate medical admissions in the state of Karnataka.[16]

---

12 Privacy In India - Country Report – October 2011, as available at http://cis-india.org/internet-governance/country-report.pdf (Last visited on 8 April 2015).

13 See *Naz Foundation v. Govt. of NCT of Delhi*, 160 Delhi Law Times 277, p. 2 (Delhi High Court 2009). The decision has been overruled by the Supreme Court of India in Suresh Kumar Koushal and another v. Naz foundation and others available at http://judis.nic.in/supremecourt/imgs1.aspx?filename=41070 (Last accessed on 9 April 2015).

14 Manjari Mishra, Aligarh Muslim University professor suspended for being gay, TIMES OF INDIA, February 18, 2010, http://articles.timesofindia.indiatimes.com/2010-02-18/india/28118769_1_shrinivas-ramchandra-sirasrickshaw-puller-amu-campus (last visited 3 Oct 2011).

15 Yogita Rao, Maharashtra colleges to install biometric card systems to check attendance - Mumbai - DNA, DNA INDIA, January 14, 2011, http://www.dnaindia.com/mumbai/report_maharashtra-colleges-to-install-biometric-cardsystems-to-check-attendance_1494247 (last visited 18 Jan 2011).

16 Biometrics Employed to Crack down on Proxies, THE HINDU, February 7, 2011, http://www.hindu.com/2011/02/07/stories/2011020756020700.htm (last visited 3 Oct 2011).

Nonetheless the understanding of right to privacy and the litigation concerning the same, in India, appears to have grown and applied in the few areas and the broader conceptualization and legal recognition of the said right is not yet apparent at least from the Indian perspective.

Part II: Privacy and Advent of Social Media

The media can possibly be best construed as a source of information for public. The transformation of human society and its manner of communication has been undergoing massive changes since inventions and innovations in the field of communication technology have been the center of human attention. Human beings as a constituting element of society had to rely mainly on the concept which can be best described as the 'social interaction' to build the society. The social interaction implies communication among its constituting elements. The society's development is invariably dependent on the standard and level of advancement of the means of communication in the society. Media has played a pivotal role in shaping the social interaction.

Over the years the human communication has passed through several stages of evolution and this process still continues. Internet as a medium of communication has revamped the face and nature of media, more particularly with the introduction of web 2.0.

Digitization has interrupted the settled environment, both socially and legally with digital mass communications technology changing the way people interact. Nowhere is this more clearly demonstrated than in the development of web 2.0, a term coined to describe this process of media/communications convergence which allows for enhanced creativity, communications, information sharing, collaboration and functionality of the web.

The kings of the new web sometimes called web 2.0, are the social media platforms content aggregators and suppliers who connect people through social groupings.[17] The lords of this new space are Bloggers, Wordpress and Twitter, for blogs and microblogs, YouTube video content and above all, Facebook for, well, just above everything.[18]

---

17 Andrew Murray, Information Technology Law: Law and Society, Second Edition, Oxford University Press, 2013, p. 112.

18 *Id*, p. 112.

These social media platforms are viewed as advantageous to the extent that it resulted in media pluralism, easy, quick and unrestricted (to a certain extent) access to information, information democratization and information disintermediation[19], all of it allowing to exercise and realize the fundamental freedom of opinion and expression.

New media has always empowered a challenge to the traditional regulatory settlement but even web 1.0 with its traditional centralized distribution model, was subject to effective regulation (to an extent). Web 2.0, though, functions de-centrally there is no moderator or gatekeeper (on most) web 2.0 sites partly due to the prohibitive costs involved. Web 2.0 sites, if they are moderated, are usually reactively moderated not protectively. They give unprecedented media distribution ability to those least able to manage it, children and young people. The dawn of the Internet and social media made communication a two-way extravaganza.[20] The cost of the printing press and broadcast tower, originally replaced in the 1990s by the cost of the PC and internet Connection, have now been replaced by a free mobile phone with video capability: in other words the cost of broadcasting is negligible.[21] These developments are the classic double edged swords. Although there a great number of positive effects to be felt of media pluralism and of web 2.0, primarily in social networking, ease of access and empowering individuals to distribute content, there are also some potentially harmful negative effects.[22] [23]

The unfavorable consequence of the new media environment that some scholars have focused on involves the decline of conventional journalistic norms. As traditional journalistic outlets shrink and blog and other internet outlets ascent to greater levels of prominence, citizens experience unfiltered news and information. Many blogs lack a traditional journalistic hierarchy in which an editor, who has the

---

19 Information is freed from the restriction of atomic carrier media. Disintermediation is where the middlemen in a supply chain are cut out. *See Id*, p. 41-44.

20 Jay Rajasekera, Crisis Management in Social Media and Digital Age: Recall Problem and Challenges to Toyota, available at http://ssrn.com/abstract=1603027.

21 *Supra* n. 18, p. 113.

22 *Id*, p. 113.

23 News reporting – many users post amateur news (video) footage which major networks may not show due to public broadcasting guidelines. A noted example is a video showing the execution of Saddam Hussein (A. Orlowski (2007), Saddam's YouTube Smash, The Register 2nd January 2007, http://www.theregister.co.uk/2007/01/02/saddam_youtube_hit/) that appeared on YouTube before major networks were able to show a sanitized version of it. Other examples are videos of beheadings or public officials caught in questionable acts.

power to withhold publication, can demand writer accountability and accuracy.[24] The journalists and bloggers have formed a relationship based not just on conflict and competition but also on codependency. They influence each other's approaches to the task of information dissemination.[25] "The effects of this on journalism are many such as acceleration of the news gathering and news reporting process. One reason bloggers can act so quickly is they do not need to take time that journalists do to produce a news story. There is no prior assignment to need to physically attend the event, no organizational layers, and no production time. Part of what makes the speed of blog coverage possible is the absence of professional standards for bloggers. Whereas journalists are trained to follow certain norms and codes of professional ethics in the construction of story, bloggers have no such guidelines. They are also free form journalistic standards of reporting. Bloggers are now also challenging journalists' watchdog role, claiming that they, not traditional journalists, are the real watchdogs because they are watching the watchdogs as well."[26]

Reporting of judicial proceedings can serve as a best instance to emphasize the hindrances in applying the standards for regulation of traditional media to the new media. In this backdrop, the contentions indentified[27] in the cases of reporting of judicial proceedings become important. Firstly, there is a professional and moral obligation on the media agencies to ensure fair and accurate reporting of court proceedings. Secondly, in some kinds of cases there is a compelling need to protect the identity and privacy of parties. The same may be required in order to ensure their security and protect their interests apart from ensuring a fair trial.

In relation to the first contention concerning media agency's obligation, the expression 'media agency' may not necessarily cover within in purview an individual stating something on her personal blog or on the wall of Facebook of her personal account. While dealing with the second contention, protecting the identity and privacy of the parties may require courts to pass certain orders such as gag orders but these orders are also targeting the media agencies and media

---

24 Richard Fox and Jennifer Ramos, iPolictics: Citizens, Elections and the Governing in the New Media Era, Cambridge University Press, 2012, p. 13.

25 Richard Devis, Politial Blogging and Journalism, in *Id*, p. 76-78.

26 *See generally Id*, p. 76-99.

27 As identified during the address by Justice K.G. Balakrishnan, Chief Justice of India, at Regional Workshop on 'Reporting of Court proceedings by media and administration of justice' at the High Court of Maharashtra and Goa, Mumbai (October 19, 2008) available at http://supremecourtofindia.nic.in/speeches/speeches_2008/19%5B1%5D.10.08_media_workshop_bombay_hc.pdf (visited on August 23, 2014).

houses and again the individual are exempted. In UK the practice by courts is issuing privacy injunctions and super-injunctions to not only protect the identity and privacy of the person involved in the matter pending before the court but also stop other people from publishing the whole issue at any forum. But even the flaws in this mechanism are evident as none of these orders could stop people from discussing such issues on a larger scale on social networking platforms all this being done in contempt of court.[28] A Joint Committee on Privacy and Injunctions was constituted immediately. The interesting outcome of the report in dealing the issue was as follows: 'Where an individual has obtained a clear court order that certain material infringes their privacy and so should not be published we do not find it acceptable that he or she should have to return to court repeatedly in order to remove the same material from internet searches. Google and other search engines should take steps to ensure that their websites are not used as vehicles to breach the law and should actively develop and use such technology. We recommend that if legislation is necessary to require them to do so it should be introduced.'[29]

There still exits a doubt as to the success and legality of such a mechanism. Though this being the scene in UK, India is completely oblivious to such developments and has not even considered the same issue seriously and this is evident from the lack of any legislative attempt to regulate the new media.

To regulate the privacy on-line the legal framework which exists in India is in the form of The Information Technology Act, 2000 (Hereinafter referred to as the IT Act). The IT Act provides for civil and criminal liability with respect to hacking (Secs 43 & 66) and imprisonment of up to three years with fine for electronic voyeurism (Sec. 66E), Phishing and identity theft (66C/66D), Offensive email (Sec. 66A). Disclosure by the government of information obtained in the course of exercising its interception powers under the IT Act is punishable with imprisonment of up to two years and fine (Sec. 72) 17 Section 72A of the IT Act penalizes the unauthorized disclosure of "personal information" by any person who has obtained such information while providing services under a lawful contract. Such disclosure must be made with the intent of causing wrongful loss or

---

28 *See* RJW& SJW v. Guardian News and Media Ltd & Persons Unknown [2009] EWHC 2540 (QB), Terry v. Persons Unknown (Rev 1) [2010] EWHC 119 (QB).

29 House of Lords, House of Commons, Report of the Joint Committee on Privacy and Injunctions available at http://www.publications.parliament.uk/pa/jt201012/jtselect/jtprivinj/273/273.pdf.

obtaining a wrongful gain and is punishable with imprisonment which may extend to 3 years or a fine of Rs. 500,000 or both.
Section 43A of the IT Act, newly introduced in 2008, makes a start at introducing a mandatory data protection regime in Indian law. The section obliges corporate bodies who 'possess, deal or handle' any 'sensitive personal data' to implement and maintain 'reasonable security practices', failing which, they would be liable to compensate those affected by any negligence attributable to this failure.

In April 2011, the Ministry of Information and Technology, notified rules[30] under Section 43A in order to define "sensitive personal information" and to prescribe "reasonable security practices" that body corporates must observe in relation to the information they hold. By defining both phrases in terms that require executive elaboration, the section and the rules in effect pre-empt the courts from evolving an iterative, contextual definition of what would count as a reasonable security practice in relation to data.

Part III: Revisiting the Concept of Privacy in the Light of Social Media

Currently, privacy is a sweeping concept, encompassing (among other things) freedom of thought, control over one's body, solitude in one's home, control over information about oneself, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations.[31]

The six different heads which can cover the general aspects of privacy are (1) the right to be let alone-Samuel Warren and Louis Brandeis's famous formulation for the right to privacy; (2) limited access to the self-the ability to shield oneself from unwanted access by others; (3) secrecy-the concealment of certain matters from others; (4) control over personal information the ability to exercise control over information about oneself; (5) personhood-the protection of one's personality, individuality, and dignity; and (6) intimacy-control over, or limited access to, one's intimate relationships or aspects of life.[32]

---

30 The Information Technology (Reasonable security practices and procedures and sensitive personal information) Rules, 2011. Available at http://www.mit.gov.in/sites/upload_files/dit/files/GSR3_10511%281%29.pdf (Last visited on15 September 2011).

31 Daniel Solove, *Conceptualizing Privacy*, 90 Cal. L. Rev. 1087 2002, at p. 1088.

32 As identified by Daniel Solove in *Conceptualizing Privacy*, 90 Cal. L. Rev. 1087 2002 at p. 1092.

If privacy is to have real meaning for the majority of users, the default settings for sharing must be limited to a close set of people.[33] The clear trend for defaults on Facebook, however, is for more and more information from users' profiles to be more and more visible as is graphically demonstrated by McKeon.[34] When even former executives of a company running a social network such as Facebook are unhappy with the privacy effects, it is hard not to conclude that the system includes neither privacy by design nor privacy by default.[35]

The issue of privacy gets more complicated when we try to understand the philosophical underpinnings of it, which indeed are essential to understand and formulate the kind of regulatory environment for protection of online privacy. The privacy now can be classified under two heads viz. privacy by obscurity and privacy by voluntary restraint.[36] Advances in information processing are eroding privacy in public. This is a problem for privacy by obscurity. A variety of technologies make it increasingly hard to hide. As privacy by obscurity declines, the need for privacy by voluntary restraint increases.[37]

Unfortunately, technology-driven business practices have already so greatly reduced privacy by voluntary restraint that we no longer move about our lives as self-contained beings, but as nodes of information production in a dense network of digital relations involving other nodes of information production. All of the data about us as individuals in social network communities is owned, operated, managed, and manipulated by third parties beyond our control, and those third parties are, typically, private companies.[38]
Keeping this conceptual analysis of privacy in mind the regulators are expected to design the legislations for the purposes of protecting online privacy. The different models which can be taken into account are (1) pragmatic approach to be adopted as suggested by Daniel

---

33 Andrew A Adam, *Facebook Code: SNS Platform Affordances and Privacy,* 23 J.L. Inf. & Sci. 158 2014, p. 163.

34 Matt McKeon, *The Evolution of Privacy on Facebook* <http://mattmckeon.com/facebook-privacy>. McKeon animated information graphic showing the expansion of default visibility of Facebook profile information from 2005-10. 2010.

35 See for detailed discussion Andrew A Adam , *Facebook Code: SNS Platform Affordances and Privacy,* 23 J.L. Inf. & Sci. 158 2014, p. 164.

36 Richard Warner, Robert H. Sloan, Self, Privacy, and Power: Is It All Over?17 Tul. J. Tech. & Intell. Prop. 61 2014, p. 65.

37 Richard Warner, Robert H. Sloan, Self, Privacy, and Power: Is It All Over?17 Tul. J. Tech. & Intell. Prop. 61 2014, p. 65, 66.

38 Ronald J. Deibert, Black Coce: Inside the Battle for Cyberspace (2011) as cited in Richard Warner, Robert H. Sloan, Self, Privacy, and Power:Is It All Over?17 Tul. J. Tech. & Intell. Prop. 61 2014, p. 66.

Solove[39], (2) modest approach to privacy protection as suggested by Woodrow Hartzog [40] and (3) the theoretical model of informational norms and protection of privacy in public as suggested by Richard Warner, Robert H. Sloan.[41] The attempt on the part of legal scholars to devise new models for privacy protection online is in itself a clear reflection of the insufficiency and ineffectiveness of the existing methods of regulation.

The Indian legal framework as explained in part I of this paper and the judicial interpretation and conceptualization of privacy is devoid of requisite philosophical and theoretical underpinnings and understanding of the different aspects of privacy.

Conclusion

The nature of media is changed with the advent of web 2.0. The traditional means of media regulations may not necessarily provide the effective regulation of this new media. There is a pressing need to have a new paradigm for the regulation in this new media environment. Mere reliance on the general laws as a means of regulation may not be of any utility. As pointed out by Lesely Hitchens,[42] the media policy and regulation will have to address the entire "media ecosystem," viewed as a "regulatory space" in which self-regulation and the market are all part of the basket of regulatory tools. The convergence of broadcasting technologies and telecommunication technologies is supposed to be addressed keeping in mind the balance to be achieved in the protection of different rights including right to privacy. Since now an individual in herself has become a broadcasting house the issues of protection of privacy of every other individual are at stake. The existing legal framework in India appears to be inadequate. The inadequacy can be safely concluded to be stemming from poor application of the developed existing scholarship pertaining to right to privacy and its various aspects. The new social media has to take steps to respect, help realize and protect the right to privacy in the light of re-conceptualization of privacy.

---

39 *See generally* Daniel Solove, *Conceptualizing Privacy*, 90 Cal. L. Rev. 1087 2002.

40 *See generally*, Woodrow Hartzog, The Value of Modest Privacy Protection in Hyper Social World, 12 Colo. Tech. L.J. 333 2014.

41 *See generally*, Warner, Robert H. Sloan, Self, Privacy, and Power: Is It All Over? 17 Tul. J. Tech. & Intell. Prop. 61 2014.

42 *See* Lesely Hitchens, Media Regulatory Framework in the Age of Broadband: Securing Diversity, Journal of Information Policy (2011):217-240.