FACEBOOK AND THE RIGHT TO PRIVACY: WALKING A TIGHT ROPE

*Arun Mal & Jenisha Parikh**

While there has been a spate of public outcry against rampant privacy violations on social networking sites in the recent past, the current law of privacy appears to be ill-equipped to reinvent itself in the internet age and rise to the emerging challenge of affording adequate protection to personal information online. This article seeks to identify the various instances of privacy abuse that have become common on social networks and explores various social and legal solutions available for redressing the same through users' protest, industry self-regulation and actions based in the law of tort, contract and data protection. In light of the limited nature of protection afforded by these alternatives, it stresses on the need to broaden and redefine the theoretical paradigm within which the right to privacy has traditionally been viewed in order to adapt it to the new avatar of social communication.

I. INTRODUCTION

In a world where many of us find that our lives have become substantially dependent on the internet and deeply tied with a number of social networking sites, it has become increasingly possible for anyone with a preliminary understanding of the workings of the worldwide web (and perhaps a credit card) to gain access to tidbits of personal information and in turn, learn a significant deal about someone one wishes to befriend, marry, employ, investigate or even stalk.[1] Unmindful of their vulnerability to such potential scavenger hunts, users hardly think twice before exposing personal information about themselves online. These tiny fragments of information, however, seldom fade away with time and therefore, are capable of being readily located and further harvested by curious individuals who possess the know how to navigate their way around social networking sites. This grim reality has evoked a vociferous, if not eye opening cry of protest from privacy advocates who have taken well to the argument that the free flow of information on the internet has, in reality, made us less free.[2] Unfortunately, however, as our world continues to change

* 3rd year and 2nd year students respectively, B.A. LL.B. (Hons.), the W.B. National University of Juridical Sciences, Kolkata.

1 Corey Ciocchetti, *Just Click and Submit*: *The Collection*, *Dissemination and Tagging of Personally Indentifying Information*, 10 Vand. J. Ent. & Tech. L. 553, 556 (2007-08).

2 Daniel J. Solove, The Future of Reputation Gossip Rumour and Privacy on the Internet 2 (2007); *See generally* Branislav Ondrasik, *Death of the "Free Internet Myth"*, 1 Masaryk U. J.L. & Tech. 7 (2007).

by the minute, lawyers, judges, legislators and legal scholars have been slow in adapting the law to tackle this dynamic and dangerous threat to privacy.[3]

One of the gravest concerns of such privacy advocates is that the proliferation of social networking sites has fundamentally challenged the common law tradition's understanding of ownership. The famous edict by John Locke that the fruits of one's labour are one's own possession, it is argued, no longer holds true in the age of Facebook and Myspace. According to the Lockean Proviso, a person who works on something can claim at least partial ownership over it.[4] This, however, does not necessarily hold true in the case of most second generation social networks where users constantly create and enhance the content available on the networks yet the information is co-opted and placed under the ownership of multinational corporations.[5] In addition, observers have also voiced concerns regarding the fact that teenagers, students and business professionals have been increasingly neutered of their desire for privacy by these social networking sites.[6] In response to these tall assertions, the social networking industry swears by the fact that their users do not really attach a very high premium to privacy in the first place and make rational privacy choices when they are online.[7]

This paper seeks to weigh these competing claims by addressing the question of how to protect privacy on social networking sites. Part II undertakes a detailed analysis of the various instances through which a user's privacy may be compromised on social networking sites. Part III analyses the legal regime that is in place to address or prevent these violations. It examines the Indian constitution's perspective of the right to privacy and the various remedies available under the law of tort, contract and data protection. An attempt is also made here to weigh the pros and cons and efficacy of users' protest and industry wide self-regulation as possible solutions to the privacy problem. Part IV calls for a need to cast a relook at the prevalent theoretical understanding of privacy as a mere right to informational self-determination in light of its inadequacies in addressing the concerns of users on social networking sites. Finally, Part V offers the concluding remarks.

---

3 Derek S. Witte, *Your Opponent Does Not Need A Friend Request To See Your Page*: *Social Networking Sites and Electronic Discovery*, 41 McGeorge L. Rev. 891 (2009-10).

4 John Locke, The Second Treatise of Government (Thomas P. Peardon ed., 1952).

5 Robert Terenzi, *Friending Privacy*: *Toward Self-Regulation Of Second Generation Social Networks*, 20 Fordham Intellectual Property, Media and Entertainment Law Journal 1049, 1064 (2010).

6 Amy Morganstern, *In the Spotlight*: *Social Network Advertising and the Right of Publicity*, 12 Intellectual Property Law Bulletin 181, 192 (2008).

7 James Grimmelmann, *Privacy as Product Safety*, 19 Widener Law Journal 795, 795-797 (2010).

II. PRIVACY RELATED CONCERNS ON SOCIAL NETWORKING SITES: POSSIBLE AREAS OF PRIVACY INFRINGEMENT

The international media had recently characterised the meteoric rise in the number of Facebook users over the past decade in very stark yet interesting terms: Facebook, it proclaimed, had become the world's third largest nation in terms of the size of its population.[8] This was, however, followed by coverage of a more unpleasant story of a security consultant who used a moderately sophisticated code to scan Facebook profiles to collect data not hidden by the users' privacy settings.[9] Soon after, the personal details of over a hundred million Facebook users were harvested and published on Pirate Bay, the world's biggest file-sharing website from where it was in turn downloaded by over a thousand users. While Facebook sharply retorted to the public outcry that followed the incident with the argument that only the information that its users had chosen to make publically available was harvested and therefore nobody's privacy had been compromised,[10] the fact remained that over a hundred million Facebook users were perhaps angry and concerned about who had access their data and what they could do with it. In another story, it was reported that a group of students from M.I.T. developed a Facebook application that claimed to be capable of surveying a user's entire profile and ascertaining whether the user was indeed heterosexual.[11] Similarly, an education major received a major setback when she lost her teaching placement and degree only because a photo of hers as a drunken pirate and an unsavoury post on MySpace was brought to the attention of her school superintendent.[12] These news reports are only a few examples of a much larger trend and underline the fact that a user's personal information has an intrinsic value and its misuse poses real and tangible risks to the user's privacy.

The unprecedented level of information sharing that takes place on social networking websites invariably has implications on personal privacy. Challenges questioning the efficacy of Facebook's infamous privacy controls have become increasingly commonplace. A vast majority of social networking sites set a particular privacy setting as default so that anyone can see a person's information unless privacy settings are actively changed. As a consequence, a

---

8 The Economist, *Facebook Population*, available at http://www.economist.com/node/16660401 (Last visited on January 27, 2011).

9 Daniel Emery, *Details of 100m Facebook Users Collected and Published*, July 28, 2010, available at http://www.bbc.co.uk/news/technology-10796584 (Last visited on January 27, 2011).

10 *Id*.

11 Dan Macsai, *MIT's Facebook "Gaydar" -Is it Homophobic?*, FastCompany, September 21, 2009, available at http://www.fastcompany.com/blog/dan-macsai/popwise/mits-facebook-gaydar-it-homophibic (Last visited on December 30, 2010).

12 *See* Snyder v. Millersville Univ., CA No. 07-1660: 2008 US Dist LEXIS 97943, at *12-22 (E.D. Pa. Dec. 3, 2008).

sizeable proportion of the users inadvertently allow public access to parts of their personally identifying information merely by failing to actively change their privacy settings.[13] This criticism is vindicated by a study that points out that 41 percent children and 44 percent adult Facebook users have open privacy settings, mostly arising out of a failure to change the default settings.[14] Critics have identified this as Facebook's underlying prejudice against privacy- sign up and it assumes you want to share as much data as possible.[15]

It may further be pointed out that even for more aware and technology savvy users Facebook's privacy controls may prove to be insufficient insofar as a significant portion of their personal data may be contained on someone else's Facebook page. For instance, a user may be tagged in a photograph or comment posted by a friend and is unable to exercise any control over how that data is presented and what privacy settings are applied by the friend.[16] Similar problems were faced with the launch of Google's social networking feature- Google Buzz. Google required Buzz users to set up public profile pages containing a list of their contacts, thereby automatically publishing a list of the user's most emailed contacts.[17] This may have been potentially hazardous for a wide variety of individuals- lawyers communicating with witnesses, cheating spouses chatting with lovers and mental health professionals issuing advice to their patients.

Yet another privacy concern is that social networking sites may retain information for unreasonably long durations. A case in point is Facebook's own terms of use that authorise it to retain any personal data in perpetuity thereby creating an irrevocable level of access to personally identifying information. Therefore, even when a user decides to exit the social network, the user's information is not within her control.[18] These concerns may be further exacerbated by the fact that more often than not social networking sites choose to retain the right to unilaterally amend their terms of use at any period of time.[19] For instance, when Facebook was first launched, only members of the

---

13 Helen Anderson, *A Privacy Wake-Up Call for Social Networking Sites?*, 20(7) Entertainment Law Review 245 (2009).

14 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 January 27, 2011).

15 The Economist, *Dicing with Data*, May 20, 2010, available at www.economist.com/node/16163396 (Last visited on January 27, 2011).

16 *Id*.

17 *See* Nicholas Carlson, *WARNING*: *Google Buzz Has a Huge Privacy Flaw*, BUS. INSIDER: SILICON ALLEY INSIDER, February 10, 2010, http://www.businessinsider.com/warning-google-buzz-has-a-huge-privacy-flaw-2010-2 (Last visited January 27, 2011).

18 Facebook, *Privacy Policy*, available at http://www.facebook.com/policy.php (Last visited on January 27, 2011).

19 Tim Wafa, *Global Internet Privacy Rights*: *A Pragmatic Approach*, 13 Intellectual Property Law Bulletin 131, 138 (2009); Jesse Perez, *Why Facebook Behaves Like an Arrogant Frat Boy*, March 25, 2009, available at http://livenews.com.au/home/why-facebook-behaves-like-an-arrogant-fratboy/2009/3/25/184829 (Last visited January 27, 2011).

social network could search for other members. A few years ago, however, Facebook announced its intention to make its limited search listings available even to people who were not logged into the network on a number of search engines.[20] With this decision, not only were the photographs and other key details of Facebook members exposed, but non-members were also able to view the list of the user's friends and send messages to the user.[21] Such terms, therefore, enable social networking sites with scant regard for users' privacy to unilaterally and recklessly alter their business models without the need to seek the users' consent.

These problems get further magnified with the recent explosion of lesser known but significantly populated second generation social networks with weak security controls. A recent example may be found in the controversy surrounding a social networking site named RockYou with a base of over thirty million users. The company was subject to loud and vociferous outrage when it was discovered that it stored the passwords of all its users in an easily accessible plain text format online. So obvious was the manner in which RockYou stored its passwords that it was accessed in its entirety by a security firm exposing the vulnerabilities of the social networking industry.[22]

Furthermore, it has been observed that the license for use of user information granted to such sites tends to be wide[23] and akin to ownership[24] to the extent that users may grant a perpetual and irrevocable license to the site as illustrated above. This may enable the site to display and distribute user information in any which way including the right to sub-license the same leaving the user with no real control.[25] The absence of express restrictions on the purposes for with social networking sites use this information makes it vulnerable to commercial exploitation. While corporations such as Facebook mandatorily require third parties who access user information (particularly developers of the myriad platform applications on the site) to bind themselves with contractual obligations protecting user privacy, guaranteed compliance by such third parties is conspicuously absent in Facebook's privacy policy.[26]

One of the major concerns that privacy activists have with regard to social networking sites is their potential to stimulate a process of unlimited

---

20 Posting of Philip Fung to The Facebook Blog, *Public Search Listings on Facebook*, available at http://blog.facebook.com/blog.php?post=2963412130 (Last visited on January 27, 2011).

21 Yasamine Hashemi, *Facebook's Privacy Policy and its Third Party Partnerships*: *Lucrativity and Liablity*, 15 B.U.J. Sci. & Tech. L. 140, 143 (2009).

22 TechCrunch, *Serious SQL Flaw Could Have Compromised Millions of Rockyou.com Users*, December 14, 2009, available at http://www.net-security.org/secworld.php? id=8612 (Last visited on January 27, 2011).

23 Ondrasik, *supra* note 2, 86.

24 Anderson, *supra* note 13, 245.

25 *Id*.

26 Anderson, *supra* note 13, 245.

information aggregation and the negative ramifications that follow from that. For instance, it is conceivable that a stalker uses his mobile phone to click a picture of a young girl and uses technologies such as tagging and facial recognition software to determine the young girl's name, residential address, hobbies and political affiliations.[27] Search engines now possess the capability to cross index a user's searches with cookies left by the websites visited by the user. This enables search engine to allow advertisers to specifically target certain goods and services. This may in turn potentially unleash a process of what has come to be known as transaction-hijacking wherein a platform may sense that a purchase is imminent and leap with an offer from a competitor offering more favourable terms.[28]

While a few may reject some of the above concerns as unreasonably farfetched and overtly sensitive, there is ample evidence from the decade long history of social networking sites to show that the fears regarding the violation of privacy on these websites are real and of daily occurrence. A case in point is Facebook's launch of an ill-fated advertising program named Beacon in November, 2007. Introduced in partnership with 44 other websites, this service posted notifications with details of the websites visited by the user on a user's Facebook page.[29] In other words, Beacon meticulously traced and updated every action undertaken by a user on an allied website and posted details regarding the same on her wall, for instance, if a user decided to purchase a personal item using eBay, details of the user's auction listings would be available for inspection by other users on the social network alongside the user's photograph, an advertising message form eBay and other related links.[30] The only way a user would be able to prevent this from happening would be if she were diligent enough to notice an unobtrusive 10 second long pop up window and had the presence of mind to click on the 'no thanks' option.[31] Even if users were quick enough to deactivate Beacon using this pop-up, they were expected to do so separately for each allied website.[32] As a result, most users were caught off guard as they viewed this message as yet another annoying pop up that didn't require their attention and privacy minded users were hit hard given that they realised what had happened only after the occurrence of the fact.[33] Simply

---

27 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).

28 *Id*.

29 *Id*., Facebook, Press Release, *Leading Websites Offer Facebook Beacon for Social Distribution*, November 6, 2007, available at http://www.facebook.com/press/releases.php? p=9166 (Last visited on January 27, 2011); *See also* Lane v. Facebook Inc., 2008 WL 3886402: No. C 08-3845 Slip Op at 1 (N.D.Cal. Oct. 23, 2009).

30 William McGeveran, *Disclosure, Endorsement and Identity in Social Marketing*, University of Illinois Law Review 1105, 1114 (2009).

31 *Id*.

32 Mike Montiero, *My Heart's in Accra*, available at http:// www.ethanzuckerman.com/blog/2007/11/15/facebook-changes-the-norms-for-web-purchasing-and-privacy/ (Last visited on January 27, 2011).

33 Grimmelmann, *supra* note 7, 803.

put, Facebook, in its trademark style, equated inactivity with regard to the pop-up window as consent by the user.[34] Critics are quick to point out that with this illusory opt out, Facebook had gone a bit too far, not only had it flouted the trust that users had placed in it with respect to their privacy, but it had provided a platform to convert their preferences into an endorsement with commercial value without seeking their full consent.[35] Moreover, Facebook started tracking user information on third party websites and announced these activities to the user's friend.[36] This is a clear example of the dangers that arise when social networking rights reserve the right to unilaterally amend their privacy policies and fail to identify any limits to the manner in which they are willing to utilise a user's personally identiying information- absolutely nothing in their past online experience would have enabled them to foretell that Facebook would adopt such a model of exposure, thereby rendering their initial consent to the privacy policy at the time of signing up to the social network meaningless.

In addition to the above, there are a large number of unintended consequences that flow from the creation of such social networks. While new technologies may be developed with honest intentions to realise a particular objective, these may be put to nefarious use by others. Given that social networks operate on open platforms, noble inventions may be used for invasive and troublesome ends from the standpoint of user privacy. In most cases, problems arise on account of the accumulation of information in such an open manner making it possible, for instance, for banks to revise a credit card holder's credit limit by amassing data on the stores at which the individual shops.[37]

Another major concern is the complexity and incomprehensible nature of the privacy policies and terms of use of most social networking sites. Among other victims of this problem was the winner of an American beauty pageant- Miss New Jersey, 2007. Under the impression that her album was restricted to her Facebook friends only, she posted some racy photographs on the site. To her utter surprise, she was soon blackmailed by another Facebook user who gained access to the album.[38] While the fault in this case may be attributed to the victim, it is not difficult to imagine that a larger number of users are left in the dark owing to the complexities of the websites complex privacy controls. Studies have consistently shown that a large majority of Facebook

---

34 Kane, *supra* note 27, 339.

35 McGeveran, *supra* note 30, 1114.

36 Juan Carlos Perez & Nancy Gohring, *Facebook Partners Quiet on Beacon Fallout*, December 12, 2007, available at http://www.washingtonpost.com/wp-dyn/content/article/2007/12/12/AR2007121200041.html (Last visited on January 27, 2011).

37 Mike Stuckey, *AmEx Rates Credit Risk by Where You Live*, *Shop*, October 7, 2008, available at http://www.msnbc.msn.com/id/27055285/ (Last visited on January 27, 2011).

38 Austin Fenner, *N.J. Miss in a Fix over Her Pics*, July 6, 2007, available at http://www.nypost.com/p/news/regional/item_u9E3QCTLwd5sD0Wz7Zb0MO (Last visited on January 27, 2011).

users have mistaken beliefs about how the company collects and shares personal information.[39]

These concerns are all the more relevant in light of the fact that a number of terms used in privacy policies tend to be plagued by hidden ambiguities. For instance, Facebook's privacy policy clearly provides that the information that the user provides the network may eventually be made 'publically available'. Most users who had signed up to Facebook in its early years would have consented to this term with knowledge of the fact that Facebook required individuals to develop a vested interest in the Facebook community by creating a profile before gaining access to information about any user. As described above, however, this practice was unilaterally reversed by Facebook without adequate notice to its users when it decided to make such information available to any member of the larger public. It has been contended by critics that the notion of 'publically available' in the pre-public search version of Facebook is substantially different from the notion of 'publically available' in the current system.[40] For this reason, sites such as Facebook have been implored to do more to explain what exactly they mean by terms such as publically available that are incorporated in their privacy policies given that users may have perhaps not consented to the terms of use had they known that such a change were to be introduced by Facebook.

III. THE SOCIO-LEGAL FRAMEFORK FOR ADDRESSING PRIVACY VIOLATIONS ON SOCIAL NETWORKING SITES

A. USERS' PROTEST

The success of the movement for the protection of online informational privacy has largely been contingent on the degree and extent to which scandals about privacy violations by social networking sites are publicised-whether in the form of a media frenzy or activism on the blogosphere.[41] For this reason, it has been argued that the only way to make legislators and perhaps more importantly, corporations take note is through a strenuous campaign of protest by the members of social networks.[42] In its early years, Facebook was

---

[39] Alessandro Acquisti & Ralph Gross, *Imagined Communities*: *Awareness*, *Information Sharing*, *and Privacy on the Facebook*, *in Privacy Enhancing Technologies*: *Sixth International Workshop*, available at http://blues.ius.cs.cmu.edu/ralph/pubs.htm (Last visited on January 27, 2011); James Grimmelmann, *Saving Facebook*, 94 IOWA LAW REVIEW 1137, 1162 (2009); *See generally* Susan E. Gindin, *Nobody Reads Your Privacy Policy or Online Contract? Lessons Learned from Questions Raised by the FTC's Action Against Sears*, 8 NORTHWESTERN JOURNAL OF TECHNOLOGY AND INTELLECTUAL PROPERTY 1-37 (2009-10).

[40] Hashemi, *supra* note 21, 149.

[41] *Id*.

[42] Morganstern, *supra* note 6, 193.

non-receptive, if not dismissive of any such movements of protest undertaken by its members. The first instance of such mobilisation of Facebook users dates back to 2006 when over three hundred thousand Facebook users protested against the News Feeds Service that had been introduced on the network.[43] In response, however, Facebook chose to let the controversy die down- not only did it decline to remove the News Feeds feature, it ensured that there was no way for members to permanently disable it. Yet another setback to the users' movement came in the form of Facebook's persistent refusal to yield to the demands of approximately seven hundred thousand protesters against its decision of opening itself to the general public.[44] Intended originally to be a platform for students from the same college to interact with each other, several members of Facebook were hesitant to forgo the campus centric college-only nature of Facebook and share information with the general public but their voices fell on deaf ears.[45] A later press release by the Vice President of Facebook is indicative of the corporation's hostility to public opinion:[46]

> "[w]henever we innovate and create great new experiences and new features, if they are not well understood at the outset, one thing we need to do is give people an opportunity to interact with them.... After a while, they fall in love with them."

With the passage of time, however, as Facebook's privacy violations became bolder and starker, the protest movement resisting the same also grew from strength to strength. The vastly unpopular decision to unveil two new services, namely Facebook Beacon and Social Ads, was ultimately reversed as over five million Facebook users signed a petition on MoveOn.org decrying the privacy infringements that these services were seen to facilitate.[47]

Sceptics have, however, pointed out that in light of the profit motive relentlessly pursued by corporations, while such a method of public shaming of companies may work in some instances, it is highly unlikely to ensure that users' demands are always met- particularly in the case of privacy

---

[43] Jamin Warren & Vauhini Vara, *New Facebook Features Have Members in an Uproar*, September 7, 2006, available at http:// online.wsj.com/public/article/SB115759058710755893-fWYkG0Idkd6hAHc0TC_xHLV9LBw_ 20070907.html?mod=tff_main_tff_top (Last visited on January 27, 2011).

[44] *See e.g.*, Facebook, *News Feed Was The Least of our Worries - People Against an Open Facebook*, available at http://facebook.com/group.php?gid=2210053630 (Last visited on January 27, 2011).

[45] *Id*.

[46] Louise Story & Brad Stone, *Facebook Retreats on Online Tracking*, November 30, 2007, available at http://www.nytimes.com/2007/l 1/30/technology/30face.html. (Last visited on January 27, 2011).

[47] Michael Liedtke, *Facebook Revamps New Advertising System*, November 30, 2007, available at http://hosted.ap.org/dynamic/stories/F/FACEBOOK_ABOUT_FACE?SITE=WIMIL&SECTION=HOME&TEMPLATE=DEFAULT (Last visited on January 27, 2011).

concerns.[48] This pessimism is perhaps justifiable on the ground that the members of social networks are adequately desensitised to losses of privacy and have become jaded to scandals- there is an outcry at first, but soon enough everything is forgotten,[49] as was the case with News Feeds and privacy concerns over the use of Gmail.

B. CONSTITUTIONAL PROVISIONS

Facebook users have argued ad nauseam for a right to privacy which is not violated arbitrarily by social networking sites. The concept of privacy, however, has intrigued many legal theorists and philosophers.[50] The goal to constitutionally define privacy remains evasive. The conceptualisation of privacy as a 'right to be left alone'[51] has been criticised as being too vague and broad. Meanwhile the conception of privacy as 'limited access to self',[52] has gained legitimacy in some quarters. Privacy as a right to determine limited access to self means that every individual has a right to decide the extent of public scrutiny and knowledge in her private life.[53] In this context, privacy has also been understood as a right to have control over one's personal information.[54]

The Supreme Court has recognised the right to privacy under Art. 21 of the Constitution through an expansive interpretation of 'personal liberty'.[55] This right, however, is not absolute.[56] The Supreme Court has held that privacy is not violated if it is intruded by a fair, just and reasonable procedure, established under law. [57] Furthermore, the Court considers other countervailing rights and interests while deciding on the issue of privacy.

In most cases privacy infringement has been alleged against the State.[58] Thus, if the right can be claimed only against the state, then the claim

---

48 Morganstern, *supra* note 6, 193.

49 *Id*.

50 Daniel J. Solove, *Conceptualising Privacy*, 90 California Law Review 1087 (2002); *See also* Arthur Miller, The Assault On Privacy: Computer, Data Bank, And Dossiers 25 (1971).

51 R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632: AIR 1995 SC 264 (The SC held that right to privacy means the right to be alone).

52 Solove, *supra* note 50.

53 *Id*.

54 *Id*.

55 Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295; Govind v. State of Madhya Pradesh, (1975) 2 SCC 148; People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301; District Registrar and Collector v. Canara Bank, (2005) 1 SCC 496.

56 Mr 'X' v. Hospital 'Z', (1998) 8 SCC 296; Vakul Sharma, *White Paper On Privacy*, available at http://iamai.in/Upload/IStandard/White%20Paper%20on%20Privacy.%202007.pdf (Last visited on January 17, 2011).

57 S*upra* note 55.

58 P.D. Shamdasani v. Central Bank of India Ltd., AIR 1952 SC 59: 1952 SCR 391; Vijaya Laxmi Tripathi v. Managing Committee of Working Women's Hostel, AIR 1976 SC 1207; Zoroastrian Coop. Housing Society Ltd. v. District Registrar, Coop. Societies (Urban), (2005) 5 SCC 632; Indu Jain v. Forbes Incorporated, IA 12993/2006 (Del) in CS(OS) 2172/2006 (High Court of

of the digital privacy stands vitiated as in most cases, the claim lies against private bodies.[59] Moreover, the Supreme Court has expressly stated that once an individual's information becomes a matter of public record, the right to privacy with respect to that information ceases.[60] Such a position bolsters Facebook's argument that users consent to make their information publically available.[61] A window of opportunity may be found in a reasonable interpretation of the term 'public domain'. It is, however, yet to be seen how far courts will be willing to go to expand the right to privacy so as to include the right to digital privacy within its purview.

C. TORT BASED ACTIONS

1. Appropriation

The tort of appropriation refers to the use of an individual's likeness for commercial ends without any prior permission on the part of such individual. Recognised in multiple jurisdictions throughout the United States, the tort of appropriation, aims at protecting an individual's privacy by affording protection to her name or likeness.[62] This tort has been given legislative recognition in California, wherein its basic ingredients include:[63]

(*a*) The defendant's knowing use of the plaintiff's name, likeness or identity

(*b*) Without the plaintiff's prior consent

(*c*) Commercial or other advantage to the defendant

(*d*) Injury to the plaintiff.

The requirements of the Californian statutory rule, however, are far more stringent than the traditional ingredients under common law. Under the tort regime, not only is knowledge on the part of the defendant an added ingredient, but it further requires that the commercial use must be directly connected with commercial sponsorship or with the paid advertising.[64] It has been pointed out that the reason for this discrepancy is the fact that whereas the common law test aims at protecting an individual's dignitary interest, the statutory

---

Delhi, October 12, 2007); *But see* V.N. Shukla, Constitution of India 211 (M.P. Singh ed., 2008) taking a contrary stand.

59 *See* Apar Gupta, *Balancing Online Privacy In India*, 6 Indian J. L. & Tech. 43 (2010).

60 *Supra* note 51.

61 McGeveran, *supra* note 30.

62 J. Thomas McCarthy, *The Rights of Publicity and Privacy*, available at http://west.thomson.com/productdetail/126362/13516725/productdetail.aspx (Last visited on January 27, 2011).

63 California Civil Code, 2007, §3344(a).

64 California Civil Code, 2007, §3344(e).

rule aims at protecting an economic interest.[65] The only defences to this tort are newsworthiness, consent, and that the individual is not identified.[66]

Online appropriation disputes have become increasingly commonplace[67] but they primarily center on the use of a domain name that users may identify with another entity.[68] From the above analysis, however, it is clear that this tort may also be resorted to for seeking damages resulting from some of the major privacy violations at the hands of social networking websites particularly, the now replaced service of Facebook Beacon. In this service Facebook clearly used the names and images of users,[69] which meets the common law requirement of 'name or likeness.' The additional statutory requirement of knowledge on the part of the defendant is also easily met in light of Facebook's own description of its advertising service.[70] The first troublesome area, however, is with respect to the existence of prior consent. Taking resort to its terms of use, Facebook may easily argue that users expressly authorised it to distribute user content for any commercial or advertising purpose in connection with the website.[71] Such a contention may, however, be addressed on the ground that the subsequent conduct of Facebook itself adverted to the fact that it felt that further consent was necessary. For instance, Facebook sought to reinitiate the process of obtaining consent using the ten second long pop-up window (which never really afforded a true opportunity to make an informed choice).[72] In fact, the C.E.O. of Facebook, Mark Zuckerberg has himself acknowledged this flaw and was quoted as saying "it took us too long after people started contacting us to change the product so that users had to explicitly approve what they wanted to share."[73] Furthermore, it has been argued that consent for some sharing in the form of acquiescence to Facebook's terms of use cannot be automatically transformed into consent for all sharing on the network

---

65 Daniel J. Solove, *Facebook and the Appropriation of Name or Likeness Tort*, available at http:// www.concurringopinions.com/archives/2007/11/facebook_and_th.html (Last visited on January 27, 2011).

66 William L Prosser, *Privacy*, 48 Cal.L.Rev. 383, 389 (1960). 405, 411-13, 419.

67 Kane, *supra* note 27, 336.

68 *See e.g.* Planned Parenthood Federation of America Inc., v. Bucci, 1997 WL 133313: No. 97 Civ. 0629, at *1 (S.D.N.Y. Mar. 24, 1997) and LLC v. Professional Pet Sitting Services, 2007 WL 1876517: No. 07-90-ST, at 1-2 (D.Or. June 26, 2007).

69 McGeveran, *supra* note 30, 1114.

70 Facebook, *Facebook Beacon*: *Enable Your Customers to Share the Actions They Take on Your Website with Their Facebook Friends*, available at http:// www.facebook.com/business/?beacon (Last visited on January 27, 2011).

71 Facebook, *Terms of Use*, available at http://www.facebook.com/terms/php (Last visited on January 27, 2011): "By posting User Content to any part of the Site, you automatically grant ... to the Company an irrevocable, perpetual, non-exclusive, transferable, fully paid, worldwide license (with the right to sublicense) to use ... publicly display ... and distribute such User Content for any purpose, commercial, advertising, or otherwise, on or in connection with the Site or the promotion thereof."

72 Morganstern, *supra* note 6, 193.

73 Mark Zuckerberg, *Thoughts on Beacon*, available at http://blog.facebook.com/blog.php?post=7584397130 (Last visited on January 27, 2011).

because in the instance of Beacon their information is used in a very different context.[74] Finally, it is not very difficult to illustrate that Beacon leads to a commercial advantage given that an endorsement by a user acts as a word of mouth promotion of a business and may be seen by friends who may subsequently acquire an interest in the product.

2. Intrusion into Seclusion

This refers to the act of physical, electronic or mechanical intrusion into an individual's life and for this tort the process of information gathering is sufficient because no publication of the same is required.[75] The tort of intrusion is very similar to that of trespass and the two are often argued simultaneously.[76] A case may be made out to argue that one cannot accumulate information about another if he/she had a reasonable expectation of privacy over that information.[77]

3. Publication of Private Facts

This tort protects an individual from having facts (even if true) published if a reasonable person would be offended at having such intimate facts about him revealed.[78] The tort is, however, inapplicable, if the plaintiff is observed in a public place or if her activities are considered newsworthy.[79]

4. Breach of Confidentiality

It has been argued that the above three privacy torts chase an unrealistic ideal- that of perfect privacy wherein absolutely no information that an individual seeks to protect may exposed to the outside world.[80] That at least a modicum of informational privacy is likely to be breached in today's highly networked world, however, is a no brainer. It is in order to address this reality with a pragmatic solution that the tort of breach of confidentiality is proposed. This tort concedes that certain breaches of privacy will inevitably take place and, therefore, focuses on the obligations owed within the chain of the breach.[81]

---

74 William McGeveran, *More Thoughts on Facebook's Social Ads*, available at http:// blogs. law.harvard.edu/infolaw/2007/11/09/more-thoughts-on-facebooks-social-ads (Last visited on January 27, 2011).

75 Andrew F. Caplan & Robert J. Donovan, *The Ethical Investigation of Fidelity Claims Protecting Privacy*, 10 Fidelity L.J. 63, 70 (2004).

76 Kane, *supra* note 27, 337.

77 *Id*.

78 *Id*.

79 Cox Broadcasting Corpn. v. Martin Cohn, 43 L ED 2d 328: 420 US 469 (1974).

80 Brian Kane, *Rethinking the Internet's Privacy Dilemma*: *A Modest Call for Informed*, *Nimble Solutions*, 20 Albany Law Journal of Science and Technology 382 (2010).

81 Lawrence M. Friedman, *Name Robbers*: *Privacy*, *Blackmail*, *and Assorted Matters in Legal History*, 30 Hofstra L. Rev. 1093, 1102 (2002).

While the above tort remedies focus on the nature of the information that is disclosed, breach of confidentiality focuses on the nature of the relationship between the person about whom the information is shared and the person sharing the information. [82] Here, a duty of confidence arises when the party subject to a duty is in a situation where it is either known or it ought to be known that the other person may reasonably expect the protection of privacy.[83] For instance, American courts have been reluctant in affording any protection to credit card holders whose purchase information is handed over by credit card companies to miscellaneous merchants on the ground that the credit card holder voluntarily provided information to the company and the independent value of such information was not recognised.[84] Had a different approach been adopted, the court would not have found it very difficult to identify the existence of a relationship behoving confidence between a customer and the company and irrespective of the nature of information passed on to the merchants, a ready remedy would be available for addressing the infringement of privacy. Therefore, it is proposed the general rules of confidence apply between users of social networking sites inter se- in a modern adaptation of *Duchess of Argyll v. Duke of Argyll*,[85] if an angry former girlfriend posts intimate or humiliating information about her boyfriend on Facebook for the world to read and watch, she may be pulled up under the tort of breach of confidence.

5. Product Liability

The concept of product liability, in nutshell, provides that if one engaged in the business of selling or otherwise distributing products, sells or distributes a defective product, he is subject to liability for harm to persons or property caused by the defect.[86] There are several benefits of bringing privacy on social networking sites within the paradigm of product liability. Firstly, one of the implications of the imposition of a duty on sellers to make their products safe is that liability may be pinned on sellers even where the accident is caused by the consumer's fault provided that a but-for[87] and a proximate causal link is in existence.[88] Therefore, even though Miss New Jersey may have been utterly careless in updating the privacy settings of her new album as described above, it would be expected under the product liability regime that Facebook should have anticipated and guarded against such an act of carelessness. Another important facet of product liability jurisprudence is that disclaimers can never be

---

82 Kane, *supra* note 27, 377.
83 Kane, *supra* note 83, 377.
84 Dwyer v. American Express Co., 3rd, 652 NE 2d 1351 (App. Court 1995).
85 1967 Ch 302: (1965) 2 WLR 790.
86 RESTATEMENT (THIRD) OF TORTS: PRODUCT LIABILITY (1998), §1.
87 The but-for test is applicable even in India: *See* International Comparative Legal Guide, Series, *Product Liability*, available athttp://www.iclg.co.uk/index.php?area=4&country_results=1&kh_publications_id=58&chapters_id=1507 (Last visited on January 27, 2011).
88 Egelhoff v. Holt, 875 SW 2d 543 (1994).

considered to be substitutes for safe products.[89] This is of particular relevance with respect to social networking sites that seek the consent of users to disclaim all responsibility for abuse.[90]

D. CONTRACT BASED ACTIONS CHALLENGING THE ENFORCEABILITY OF PRIVACY POLICIES AND TERMS OF USE AGREEMENTS

Given that the privacy policies of most social networking sites aim at disclaiming any form of liability and giving websites the maximum possible freedom with respect to the use of the users' personal information, privacy policies more often than not prove to be unfavourable contracts binding consumers leaving them with little or no leeway in seeking legal action against the site. As a result, consumers are likely to seek to challenge and not enforce the binding effect of such policies.[91] The various challenges that may be raised against this include the absence of free consent, unconscionable terms and illusory and unenforceable nature.

The most obvious challenge to the enforceability of the privacy policies of social networking sites is the absence of free consent. A contract is enforceable only if both the parties to it have manifested their full and free consent to all its terms.[92] Recent authorities suggest that users are bound only to such online agreements that compulsorily require them to view the agreement in their totality in order to complete a transaction and click on the terms- 'I Agree' (clickwrap agreements), a process that is commonly used for the installation of new software.[93] On the other hand, license agreements that are only visible to the user by scrolling down the screen and are not required to be viewed by users in their entirety do not enjoy the same assurance of enforceability.[94] American jurisprudence is replete with authorities to the effect that merely requiring a user to click on a space to signify acceptance is not sufficient if the user is not compelled to view the agreement for the application to be processed.[95] This precise question came up for the consideration of the court

---

89 Grimmelman, *supra* note 7, 26.

90 *See* Facebook, *Statement of Rights and Responsibilities*, available at http://www.facebook.com/terms.php (Last visited on January 27, 2011): "We are providing facebook 'as is' without any express or implied warranties ... Our aggregate liability arising out of this statement or facebook will not exceed the greater of one hundred dollars ($100) or the amount you have paid us in the past twelve months."

91 Allyson W. Haynes, *Online Privacy Policies*: *Contracting Away Control Over Personal Information*, 111 Pennsylvania State Law Review 587, 624 (2006-07).

92 Indian Contract Act, 1872, §10.

93 Mark A. Lemley, *Terms of Use*, 91 Minn. L. Rev. 459 (2006).

94 Specht v. Netscape Communications Corpn., 150 F Supp 2d 585.

95 Comb v. Paypal Inc. 218 F. 2d 1165; Strujan v. AOL, No. 055175/05, 2006 WL 1452778 (N.Y. Civ. Ct. May 19, 2006; Williams v. America Online Inc., No. 00-0962 2001 WL 135825 (Mass Super Ct. Feb 8, 2011). Comb v. PayPal Inc., 218 F Supp 2d 1165; Strujan v. AOL, No.

in *Re*: *Northwest Airlines Privacy Litigation*,[96] wherein it held that "... absent an allegation that plaintiffs actually read the privacy policy, not merely the general allegation that plaintiffs 'relied on' the policy, plaintiffs have failed to allege an essential element of the contract claim: that the alleged 'offer' was accepted by plaintiffs." The finding that broad policy statements made by a website do not generally give rise to contract claims has been subsequently reinforced.[97] Therefore, if users are deemed to have consented to Facebook's privacy policy by virtue of their membership to the social network, the consumer may take resort to this argument to contend that no binding contract was entered into because true assent was never given in a true sense.

A case has also been made by several scholars to argue that a social networking site's terms of use and privacy policy may be struck down on grounds of being both procedurally and substantively unconscionable.[98] The first aspect i.e. an unfair process of entering into the contract may be contended on grounds of the standard form, undue length, fine print, misleading terms, confusing language and unequal bargaining positions that characterise the contract between Facebook and its users.[99] The argument of procedural unconscionability may be strengthened by the fact that there is no way for users to bargain with Facebook for alterations to the terms before consenting to a manifestly unfair contract and the company's unilateral right to amend the terms of the policy. Furthermore, the one-sidedness of the arbitral clause that forms a part of the privacy policy may further be plead as a ground of substantive unconscionability.[100] Using the logic in *Defontes* v. *Dell Computers Corp*.,[101] it may be argued that the arbitration clause is substantively unconscionable because its language was so one-sided as to render it an unenforceable and illusory promise, again, because of the company's unfettered right to amend the same.[102] Another related argument may be the unreasonableness and inconvenience caused to global users with regard to the forum selected for litigation,[103] which in Facebook's case is Santa Clara county in California.[104] Using largely the same arguments, courts have ruled that the arbitration clause in a clickwrap

055175/05: 2006 WL 1452778 (N.Y. Civ. Ct. May 19, 2006; Williams v. America Online Inc., CA No. 00-0962: 2001 WL 135825 (Mass Super Ct. Feb 8, 2011).

96 No. Civ. 04-126(PAM/J SM): 2004 WL 1278459 (D. Minn. June 6, 2004).

97 Dyer v. Northwest Airlines Corp., 334 F. Supp. 2d 1196 (D.N.D. 2004).

98 Hashemi, *supra* note 21, 157; Haynes, *supra* note 91, 618.

99 Hashemi, *id*.

100 Circuit City Stores Inc. v. Adams, 279 F 3d 889 (9th Cir 2002); Ticknor v. Choice Hotels Int'l Inc., 265 F 3d 931; Armendariz v. Foundation Health Psychare Services Inc., 6 P 3d 669 (2000); Bellsouth Mobility LLC v. Christopher, 819 So 2d 171 (Fla. Dist. Ct. App. 2002); Iwen v. United States West Direct Inc., 977 P 2d 989 (Mont. 1999); Burch v. Second Judicial Dist. Court of Nevada, 49 P 3d 647 (2002).

101 No. C.A. PC 03-2636, 2006 WL 253560 (R.I. Super January 29, 2004).

102 *See* Morrison v. Amway, 517 F.3d 248 (5th Cir. 2008).

103 Haynes, *supra* note 91, 618.

104 Facebook, *Terms of Use*, available at http://www.facebook.com/terms.php?ref=pf (Last visited on January 27, 2011).

agreement entered into between a Facebook user and a website affiliated to the Beacon program was unconscionable, and thereby unenforceable.[105]

E. DATA PROTECTION

Unlike the United States or the European Union, India does not have a comprehensive statute for data protection and digital privacy.[106] The provisions of the Information Technology Act, 2000 ('the Act') have long been considered inadequate to deal with privacy claims of the sort that have become common in light of the proliferation of second generation social networking sites.[107] The first hurdle created by the Act is its narrow and restrictive definition of the term 'data' which requires it to be prepared in a formalised manner.[108] The scope of such formalisation, however, remains ambiguous and *prima facie* does not cover user data available informally on social networking sites.

While the passage of the Information Technology (Amendment) Act, 2008 ('the Amendment') has been hailed by some commentators as a step in the right direction and "enough to make corporate bodies start acting to implement and maintain internal security procedures",[109] this paper maintains that the Amendment is a damp squib. For instance, the newly added §72-A punishes the disclosure of information in breach of a lawful contract with imprisonment or fine.[110] The section's insistence on establishing intent to cause wrongful gain/loss without consent, however, is akin to shooting the plaintiff in the foot given that the very nature of the contracts concluded between users and social networking sites is such that the latter are provided unbridled access over the information disclosed by the former.

Another important provision in the Amendment is §43-A which provides for the payment of compensation in case of a failure to protect any

---

105 Harris v. Blockbuster Inc., 622 F Supp 2d 396 (ND Tex 2009), 400 (2009).

106 Madhavi Divan, *The Right to Privacy in the Age of Information and Communications*, (2002) 4 SCC (Jour) 12.

107 Sharma, *supra* note 56.

108 §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.

109 Raj Lonsane, *Section 43A of the Information Technology* (*Amendment*) *Act*, *2008*, available at http://www.workoninternet.com/business/working-online/security/32035-information-technology.html (Last visited on May 20, 2011).

110 §72-A: Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both.

sensitive personal data by a body corporate.[111] While the Amendment's conspicuous silence over any upper limit for compensation is welcome, it is pertinent to note that in order to be entitled to any relief the plaintiff is expected to prove that there was negligence on the part of the body corporate in maintaining reasonable security practices. Moreover, it is submitted that the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ('the Rules') made under Explanations (ii) and (iii) to §43-A render the provision toothless. The first proviso to Cl. 3 of the Rules excludes 'any information that is freely available or accessible in public domain' from the category of sensitive personal data, thereby virtually exempting social networking sites from liability. Against this backdrop, it is questionable how useful subsequent clauses mandating clear privacy policies,[112] written consent for collection of sensitive personal data,[113] non-retention of sensitive personal data for a term longer than is required,[114] options for withdrawal of consent[115] and prior permission before disclosure to third parties[116] will be for users of social networking sites.

Finally, the Personal Data Protection Bill, 2006 (the 'Bill') was tabled before the Parliament with the objective of protecting personal data collected by the government or any private individual from commercial exploitation. Although the Bill was introduced almost five years ago, it has still not seen the light of the day.[117] Moreover, the definition of personal data, does not explicitly mention user information available over the internet. This may prove to be a major setback to litigants seeking to protect personal data. [118]

F. INDUSTRY SELF-REGULATION

It is arguable that social networking sites have an inherent incentive in facilitating the process of protecting users' data. Given that a critical mass is the first pre-requisite for the success of any social network, the number of users participating in it is its most formidable asset. A wide user base not only facilitates popularity but also plays a vital role in maximising revenues because the volume of advertisements and licensed content is a direct function of the

[111] §43-A: 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.

[112] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Clause 4.

[113] *Id*., Clause 5(1).

[114] *Id*., Clause 5(4).

[115] *Id*., Clause 5(7).

[116] *Id*., Clause 6.

[117] Subhajit Basu, *Policy Making, Technology and Privacy in India*, 6 INDIAN J. L. & TECH. 65 (2010).

[118] Personal Data Protection Bill, 2006, §2(c).

size of the audience to the website. At the same time, it is imperative for such sites to create an environment where in participation in the network is viewed as a personal experience for users instead of the disclosure of information to a commercial undertaking. Add to that the potential loss of reputation that may be caused to sites such as Facebook or Myspace were its privacy policy to become infamous for privacy infringements and the logic for incentive for self-regulation becomes apparent.[119] This logic may, however, be turned on its head with equal ease. It is becoming increasingly clear that in several cases those who assert a privacy interests are the same individuals who publicise personal information on the internet.[120] This disconnect between privacy interests and information sharing makes self-regulation on the internet implausible.[121]It has, however, been argued that the internet's solid tradition of self-regulation and letting user preferences motivate the correction of security deficiencies flies in the face of such pessimism.[122] It is clear that there is no way for social networking applications that seek to exploit and abuse private information for vested commercial interests to outdo others that have a strong reputation for protecting privacy as the latter will attract more customers. The fact that internet users are no longer willing to let social networking giants steamroll their privacy concerns is evident from the widespread hue and cry that forced Facebook to relent on features such as Beacon and Google to introduce changes to Buzz. Lessons have indeed been learned- second generation start-up social networking sites such as YingYang and Friend Feed have made efforts to make their privacy policies clear and easier to understand by adding bullet points and highlighting the most important provisions.[123] Yet another argument that is often advanced in support of the case of industry self-regulation is the fact that the Parliament lacks the means to keep pace with the level of innovation over the internet and ever evolving methods of information sharing on social networking sites.[124]

The most honest attempt towards self-regulation has perhaps been undertaken by Google. Google, as a matter of policy, anonymises all the user information that it accumulates making it impossible to trace the information to any specific or individual user when such information is shared across application programming interfaces.[125] This was followed by the launch of another initiative named Privacy Dashboard which contains an exhaustive list of all the user's applications and enables her to set privacy preferences for each

---

[119] Anderson, *supra* note 13, 245.

[120] *See generally* Face of Danger: Facial Recognition and the Limits of Privacy Law, 120 HARV. L. REV. 1876 (2007).

[121] Kane, *supra* note 27, 335.

[122] Terenezi, *supra* note 5, 1099.

[123] *Id*.

[124] Terenezi, *supra* note 5, 1099.

[125] Google, *Google Privacy Center*, available at http:// www.google.com/privacy.html (Last visited on January 27, 2011).

application separately.[126] To this extent Google seeks to assuage fears and earn the trust of the internet community by placing heavy reliance on encryption and anonymising techniques.

In spite of these promising trends, however, it is understandable that the inherently 'social' nature of social networking sites means that self-regulation of a database is insufficient and sometimes even counterproductive if carelessly handled, thereby making industry self regulation a half myth.[127]A perennial discrepancy between the amount of privacy that users expect and the amount of privacy that social networking sites are willing to offer them results is creating a market failure.[128] Users tend to overestimate how much privacy they will get as a result of which they fail to negotiate for enough. The economically rational response for a social networking site is, therefore, to undersupply it.[129] This gap manifests itself in the sense that users hardly account for privacy settings before they begin to share information on these networks and websites change their architecture to defeat earlier privacy expectations.[130] In many cases, the people whose privacy is at stake are not even in a position to effectively negotiate the optimal level of privacy with the website- as in the case of photographs tagging non-users of the website.[131] The major reason why industry self-regulation is doomed to failure in most cases is because of the absence of an essential pre-requisite for the success of market forces- stable privacy preferences. Not only do individuals feel the need for greater privacy as they age (once they are already members of the social network) but also as the network itself ages and more and more people become members.[132]

The above analysis clarifies that while it may at times be in the best interest of social networking sites to regulate themselves with a view to protect users' privacy, there also exist adverse economic incentives and the possibility of market failure. Governmental and Judicial regulation of privacy standards may have its limitations but it would be unfair to argue that it should abdicate this field of regulation in its entirety.

---

126 Erick Schonfeld, *Google Gives You a Privacy Dashboard to Show Just How Much It Knows About You*, November 5, 2009, 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 January 27, 2011).

127 Grimmelmann, *supra* note 7, 797.

128 Grimmelmann, *supra* note 39, 23.

129 *Id*.

130 Jonathan L. Zittrain, *The Generative Internet*, 119 Harv. L. Rev. 1974, 1980-96 (2006).

131 *Id*.

132 Anupam Chander, *Youthful Indiscretion in an Internet Age* in Privacy and Free Speech on the Internet (Martha Nussbaum & Saul Levmore eds.) (On file with the Iowa Law Review).

IV. REDEFINING THE THEORETICAL UNDERSTANDING OF PRIVACY IN THE INTERNET AGE

Privacy, as above, has most often been conceived as an individual's personal right to control the use of her data. Touted as 'informational self-determination', this autonomy based approach attaches a high value to placing an individual at the centre of decision-making with regard to the use of personal information. Under this theoretical paradigm, the distinctions between information and property are blurred and information is sought be isolated from free access. Therefore, by commoditising information, the idea of information self-determination proposes an intellectual property regime for the protection of privacy.[133] This notion of information self-determination as a pre-existing quality may, however, be subject to challenge by limitations on choice-making by individuals primarily on the ground that most users are usually unaware of the fact that the websites they visit collect their information and process it for varied purposes.[134] Furthermore, if the only tool that individuals are empowered with is the autonomy to decide how their information is to be used, they would often accept whatever the industry offers them because of the largely standardised form of online privacy policies. Vesting individuals with the right to self determination in light of their propensity to choose default terms because of the lack of a better alternative is an inadequate, if not superficial, alternative for the protection of privacy. Against this backdrop, the only real choice being offered to a privacy minded user is to abandon cyberspace altogether. Another key consideration is that with the proliferation of third party involvement in social networking sites, a significant part of personal information use online is removed from the two party realm of the user and the service provider. The problem, however, does not end here. A diabolical flaw in the privacy-as-autonomy model is its predisposition to commodify information and view it as something that may be traded in a privacy market.[135] All this approach does to protect privacy is to give an individual an entitlement over her personal information but is this enough?

The clear alternative to the information self-determination approach of viewing privacy is to view privacy as a constitutive value i.e. access to personal information and limits on it help in the very formation of the society that we form a part of and shape our individual identities. The fact that information privacy is important for both individuals as well as the community as a whole makes it necessary to concentrate one's attention on the boundaries of personal information. Consequently, the constitutive view is a process of

---

[133] Paul M. Schwartz, *Internet Privacy and the State*, available at http://papers.ssrn.com/sol3/papers.cfm ?abstract_id=229011 (Last visited on January 27, 2011).

[134] *Id*.

[135] *Id*.

line drawing to ascertain the permitted levels of scrutiny. In other words, the constitutive view of privacy seeks to define information territories which in turn create patterns of knowledge or ignorance of personal data stimulating and/or discouraging different levels of access to information.[136] The argument is essentially that the former approach that seeks to maximise secrecy about an individual's pursuits is unwarranted and should done away with in favour of a more dynamic approach of creating data preserves that protect personal information from different forms of intrusion. A pertinent point is that this approach does not argue for banishing the notion of self-determination from an understanding of privacy, it merely argues that in light of the changes ushered in by the internet age, it can no longer be viewed as its only component. This constitutive approach goes a step further from the first theory by painting a much broader vision of privacy- access to personal information and limits on it help form society. This, the theory argues, can only be achieved if the state plays a proactive role in the regulation of the internet.[137]

The constitutive theory of privacy comes very close to a dignity-focused view of privacy in which privacy encompasses the right of an individual to keep certain aspects of his life unknown to the public and thereby construct different situational personalities. Consequently, an individual maintains multiple public personas each of which are accessible by different constituencies and in different contexts.[138] Given that mere control over information alone is insufficient, it is arguable using the dignity based approach that all sensitive information should be kept within the social network irrespective of what is source may be. To that extent, such an understanding addresses the problems associated with third party liability and plugs the gaps in the information self-determination model.

V. CONCLUSION

A vast majority of social networking sites seem to have inculcated a prejudice against users' privacy, whether it be in the form of unreasonable default settings, insufficient privacy controls, data retention, third party abuse or a unilateral right to amend privacy policies. The attempt here is perhaps to acquire a wide and irrevocable right of ownership over a user's information and use the same for vested corporate interests such as advertising. The possibility of data aggregation further poses several real threats to the privacy of users while corporations such as Facebook are increasingly seen either turning a blind eye to such concerns or shrugging them off as unreasonable and unrealistic.

---

[136] *Id*., *See also* Fred H. Cate, *Principles of Internet Privacy*, 32 CONNECTICUT LAW REVIEW 877 (2000).

[137] Schwartz, *supra* note 120.

[138] Avner Levin & Patricia Sánchez Abril, *Two Notions of Privacy Online*, 11 VANDERBILT JOURNAL OF ENTERTAINMENT AND TECHNOLOGY LAW 1001 (2008-09).

While widespread media attention, user protest and self-regulation have achieved some modest results, it is abundantly clear that the law needs to step in to actively ensure the prevention and punishment of privacy violations by social networking sites. Given the reluctance of Indian courts in expanding the ambit of the right to privacy to protect even publically available information from being misused and the conspicuous silence of the country's data protection laws, the only alternative is to take resort to the law of tort and contract to address a user's concerns. While various privacy torts such as appropriation, breach of confidentiality and product liability apply directly to the cases under consideration, it may also be beneficial to challenge the enforceability of privacy policies and terms of use agreements on grounds of unconscionability and lack of free consent. The availability of such common law reliefs, however, does not undermine the need for a comprehensive legislation to address these concerns.

Attempts to seek an effective legal redress to privacy violations, however, will remain hollow unless a concerted effort is made to redefine the theoretical paradigms within which we view the right to privacy. The limitations of the information self-determination model can only be plugged if a dignity centric view of privacy is adopted to protect sensitive information irrespective of its source.