RIGHT TO PRIVACY AND DIGITAL AGE IN INDIA

Vishal Karnani

ICFAI Law School, ICFAI University, Jaipur

The natural human need for communication and socialization is the reason for the ever-increasing use of social networking services. These sites provide the young users the opportunity to mingle with a huge network of familiar as well as anonymous friends with over more than one billion users connected through online social media, user privacy is becoming even more crucial and is widely argue in the media and researched in academic world. Social network application provider's benefit from the increasing amount of personally detectable information keenly displayed on their sites but, at the same time, risks of data exploitation threaten the information privacy of individual users as well as the providers. Safeguard and preventative methods are not very difficult, but one need to be careful while he is on the Internet, the access permission should be given only to those applications which one are trust worthy. This paper is an attempt to understand varies factors, especially Indian laws on privacy and privacy awareness which may influence users to recognise the extent of date which should be disclose online and the concept of information protection in online environment, this paper make an effort to consolidate the different views on privacy behaviour from the perspectives of privacy protection and information disclosing.

Keywords – *Socialization, Social networking services, Social network application, Privacy awareness.*

INTRODUCTION

"There are no private lives. This is the most important aspect of modern life. One of the biggest transformations we have seen in our society is the diminution of the sphere of the private. We must reasonably now all regard the fact that there are no secrets and nothing is private. Everything is public."

-Philip K. Dick[1]

If one feels like someone is watching him, he is correct. If you're worried about this, you have plenty of company. If you're not doing anything about this anxiety, you're just like almost everyone else.'[2]

[1] Philip Kindred Dick (December 16, 1928 – March 2, 1982) was an American science fiction writer.
[2] Bob Sullivan, 2011

Social networks are a very influential communications tool that also has the ability of accumulating large volumes of info. However, if this user-related information is exploited in certain ways, it can have harmful consequences on user privacy. With social networking It has become like an practice for the adults to create online profiles and undoubtedly they are hooked to mobile phones, laptops and PCs. Accessing the internet through the mobile phones has made it even more easier for the youngster to get logged-in into Facebook, tinder, snapchat, whats app or Twitter most of the time and post updates about their daily activities. Sharing in the social networking sites and having an increased number of friends on the list is supposed to be a trend that cannot be ignored in any way. Nonetheless, the so called 'friend list' also includes some mysterious friends and sharing of thoughts or private stuffs to them might not be a decent idea. Social networking sites offer privacy measures and encourage sharing of personal information.

Moreover, social network sites is now being connected with users' physical locations, permitting information about users' preferences and social relationships to interact in real-time with their physical environment. This fusion of online social networks with real-world mobile computing has created a fast growing set of applications that have unique requirements and unique implications that are not yet fully understood. LAMSN systems such as WhozThat [3] and Serendipity [4] provide the infrastructure to leverage social networking context within a local physical proximity using mobile smart phones. However, such systems pay little heed to the security and privacy concerns associated with revealing one's personal social networking preferences and friendship information to the ubiquitous computing environment.

Although Online social networking offers a new, easy and inexpensive way to maintain already existing relationships and present oneself to others but the increasing number of actions in online services also gives a rise to privacy concerns and risks. As Social networking sites have a lot of users who have "an open profile" with considerable amount of personal information e.g. photos, location, contact information, current "whereabouts status", and so on. Do these users feel comfortable with sharing all their personal information with a large number of strangers? Or do they actually know who can access their profile information? Are they concerned about their privacy?

PRIVACY

Privacy defined

There is no recognized definition of confidentiality in academia or in government circles. Over the course of time several definitions have been gone in to. In this field we look into

[3] A. Beach, M. Gartrell, S. Akkala, J. Elston, J. Kelley, K. Nishimoto, B. Ray, S. Razgulin, K. Sundaresan, B. Surendar, M. Terada, and R. Han, "Whozthat? evolving an ecosystem for context-aware mobile social networks," IEEE Network, vol. 22, no. 4, pp. 50–55, July-August 2008.

[4] N. Eagle and A. Pentland, "Social serendipity: Mobilizing social software," IEEE Pervasive Computing, vol. 4, no. 2, April-June 2005.

some of those definitions. One of the first definitions of confidentiality, by Aristotle, makes a distinction between political activity as public and family as private [5].Implied here are barrier that might be suggested by the walls of a family house, an assumption which is made explicit, though also modified, in a far more recent definition, that of Associate Justice John Paul Steven of the US Supreme Court.[6] Here, "*the home is not the exclusive locus of privacy, but is, rather, the informing image or design in light of which privacy in other contexts may be interpret".* This is an interesting definition. The Internet has managed to dim the boundaries that would have been suggested by the walls of a house.

William Parent provides a definition of privacy which does not rest on an implicit physical dimension, as follows:[7]

"Privacy is the condition of not having undocumented personal knowledge about one possessed by others. A person's privacy is subside exactly to the degree that others possess this kind of knowledge about him"

According to Black's Law Dictionary:

"*Right to be let alone; the right of a person to be free from any unwarranted publicity; the right to live without any unwarranted interference by the public in matters with which the public is not necessarily concerned*".

Privacy concerns demand that user profiles never publish and mete out information over the web. Variety of information on personal home pages may contain very sensitive data such as birth dates, home addresses, and personal mobile numbers and so on. This info can be used by hackers who use social engineering practices to get benefits of such sensitive information and steal money.

Recently, On the 24th of August 2017, a nine-judge bench of the Supreme Court delivered its verdict in ***Justice K.S. Puttaswamy* v. *Union of India***[8], unanimously affirming that the right to privacy is a fundamental right under the Indian Constitution. It was held that:

"Privacy includes at its core the preservation of personal intimacies, the sanctity of family life, marriage, procreation, the home and sexual orientation. Privacy also connotes a right to be left alone. Privacy safeguards individual autonomy and recognises the ability of the individual to control vital aspects of his or her life. Personal choices governing a way of life are intrinsic to privacy. Privacy protects heterogeneity and recognises the plurality and diversity of our culture. While the legitimate expectation of privacy may vary from the

[5] Privacy: Stanford Encyclopedia of Philosophy, 2002.

[6] Manaster, Kenneth A. (2001), Illinois Justice: The Scandal of 1969 and the Rise of John Paul Stevens, Chicago: University of Chicago Press, ISBN 0-226-50243-0

[7] William A. Parent, "A New Definition of Privacy for the Law," Law and Philosophy 2 (1983) 305-338; "Privacy, Morality, and the Law," Philosophy and Public Affairs 12 (1983), 269-288. Page references to these articles will be given in parentheses using "LP" and "PPA" respectively.

[8] WRIT PETITION (CIVIL) NO 494 OF 2012. Decision on August 2017

intimate zone to the private zone and from the private to the public arenas, it is important to underscore that privacy is not lost or surrendered merely because the individual is in a public place. Privacy attaches to the person since it is an essential facet of the dignity of the human being"

Privacy is important because it helps people maintain their independence. Controlling the publicity of information about themselves essentially helps them in defining themselves and in a free country they would certainly not have to answer questions about the choices they make or the information they share.

SOCIAL NETWORKING

The increasing complexity of information technology with its capacity to collect, analyse and publish information is posing significant threats to social networks users privacy. It is now common wisdom that the power, capacity and speed of information technology are accelerating rapidly. The extent of privacy invasion or certainly the potential to invade privacy increases correspondingly.[9]

Ambient location sites, Photo sharing sites, video sharing sites, geolocation networks, blogs, microblogs, curation sites- trying to understand the essence and characteristics all of these different types of social network sites can feel like trying to understand or explain rocket science. Many social networks can be broken up into many categories and most networks fall into more than one category[10]. The present paper is outlining the 3 most daily used social networking sites giving examples and characteristics in order to understand the spectrum of the issue with social network privacy.

Every minute of the day[11]:

- 100,000 tweets are sent
- 684,478 pieces of content are shared on Facebook
- 2 million search queries are made on Google
- 48 hours of video are uploaded to YouTube
- 47,000 apps are downloaded from the App Store
- 3,600 photos are shared on Instagram
- 571 websites are created
- $272,000 is spent by consumers online[12]

[9] Privacy and Human Rights, An International Survey of Privacy Laws and Practice. Global Internet Liberty Campaign. Available at: http://www.gilc.nl/privacy/survey/intro.html. Retrieved on 10/Nov./2017 Time 01:30 PM

[10] McIntosh, K. (2012) Different Types of Social Media. Social-Ology. Published on March 6. Available at: http://kevinmcintosh.com/social-media-marketing/different-types-of-social-media/ Retrieved on 10/Nov./2017 Time 01:40 PM

[11] (Source: thesocialskinny.com)

[12] (source: All Twitter)

PRIVACY IN SOCIAL NETWORKS

Privacy Paradox

The "Privacy Paradox" is a phenomenon that occurs when individuals, who state that they have concerns about their privacy online, take no action to secure their accounts.[13] Furthermore, while individuals may take extra security steps for other online accounts, such as those related to banking or finance, this does not extend to social media accounts. Some of these basic or simple security steps would include deleting cookies, browser history, or checking one's computer for spyware.[14] Some may attribute this lack of action to "third-person bias". This occurs when people are aware of risks, but then do not believe that these risks apply or relate to them as individuals. Another explanation is a simple risk reward analysis. Individuals may be willing to risk their privacy to reap the rewards of being active on social media. Often times, the risk of being exploited for the private information shared on the internet is overshadowed by the rewards of exclusively sharing personal information that bolsters the appeal of the social media user[8].

Location Based Social Networks and Privacy

Location based social networks are part of what is called Location based services (LBS). They are made possible by linking Global positioning system (GPS), which track user's location, to the capabilities of the World Wide Web, along with other vital features such as instant messaging.

Location-Based Social Networks (LBSN) derives from LBSs and is often referred to as Geosocial Networking. As reported in Microsoft Research "*a LBSN does not only mean adding a location to an existing social network so that people in the social structure can share location-embedded information, but also consists of the new social structure made up of persons connected by the interdependency derived from their locations in the physical world as well as their location-tagged media content, such as photos, video, and texts*" [15] Further, the connection between users goes beyond sharing physical locations but also involve sharing knowledge like common interests, behaviour, and activities.

INDIAN LAWS & PRIVACY ON SOCIAL NETWORKING

India Need Clarity and Codification

[13] Gross, R. and Acquisti, A. 2005. Information Revelation and Privacy in Online Social Networking Sites (The Facebook Case).[online]. p. 2. Available at: http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf Retrieved on 10/Nov./2017 Time 02:30 PM

[14] Gaudeul, Alexia; Giannetti, Caterina. "The effect of privacy concerns on social network formation". *Journal of Economic Behavior & Organization*. **141**: 233–253.

[15] Microsoft (2012) Location based social networks. Retrieved from http://research.microsoft.com/en-us/projects/lbsn/ Retrieved on 11/Nov./2017 Time 04:30 PM

The conflict of laws in cyberspace has further widened the law enforcement access deficit that India is presently facing. Most of the law execution agencies of India openly admit that when the server of a website is located outside India it becomes next to difficult to prosecute a cyber-criminal using such a website and committing an offence against Indian citizen. Currently, India's most comprehensive legal provisions that speak to privacy on the internet can be found in the Information Technology Act (ITA) 2000. The ITA contains a number of provisions that can, in some cases, protection online secrecy, or in other cases, dilute online privacy. Provisions that clearly protect user privacy include: penalizing child pornography,[16] penalizing, hacking and fraud[17] and defining data protection standards for body corporate.[18]

Provisions that serve to dilute user privacy speak to access by law enforcement to user's personal information stored by body corporate[19] collection and monitoring of internet traffic data[20] and real time monitoring, interception, and decryption of online communications.[21] Additionally, legislative gaps in the ITA serve to weaken the privacy of online users. For example, the ITA does not address queries and situations like the evidentiary status of social media content in India, merging and sharing of data across databases, whether individuals can transmit images of their own "private areas" across the internet, if users have the right to be notified of the presence of cookies and do-not track options, the use of electronic personal identifiers across data bases, and if individuals have the right to request service providers to take down and delete their personal content.

The Report of the Group of Experts on Privacy

On October 2012 the Report of the Group of Experts on Privacy was published by a committee of experts chaired by Justice A.P. Shah.[22] The report creates a set of recommendations for a privacy framework and legislation in India. Most significantly, the Report recognizes privacy as a fundamental right and defines nine National Privacy Principles that would apply to all data controllers both in the private sector and the public sector. This would work to ensure that businesses and governments are held accountable to protecting privacy and that legislation and practices found across sectors, states/governments, organizations, and governmental bodies are harmonized. The privacy

[16] ITA section 67
[17] ITA section 43, 66, and 66F
[18] Information Technology (Reasonable security practices and procedures and Sensitive personal data or information) Rules, 2011.
[19] Information Technology (Reasonable security practices and procedures and Sensitive personal data or information) Rules, 2011. section 6(1)
[20] Information Technology (Procedure and Safeguards for monitoring and collection of Traffic Data or other information) Rules 2009
[21] Information Technology (Procedure and Safeguards for intercepting, monitoring, and decryption) Rules 2009
[22] Report of the Group of Experts on Privacy. Available at: http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf Retrieved on 10/Nov./2017 Time 07:30 PM

principles are in line with global standards including the EU, OECD, and APEC principles on privacy, and include: notice, choice & consent, collection limitation, purpose limitation, access and correction, accountability, openness, disclosure of information, security. India does not have any separate law which is designed exclusively for the data protection. Nevertheless, the courts on several cases have interpreted "data protection" within the ambits of "Right to Privacy" as implicit in Article 19 and 21 of the Constitution of India. However, the Ministry of Electronics and Information Technology (MeitY) has appointed an expert group headed by former Supreme Court judge BN Srikrishna to draft a data protection law.

WHAT CAN BE DONE?

The more multifarious social networking sites may need to be looked at from a law administration perspective. Some questions should be addressed including:

- Can a crime be committed in a virtual world?
- Under whose jurisdiction might this fall?
- Can evidence of a crime be gathered in a virtual world? What will be regarded as legally admissible evidence?
- Is a debate between avatars in a virtual world legally perceptible, either as a basis of a business deal or as a meeting of terrorist/criminal individuals?

From a corporate perspective, a revised security model which takes into account the sharing of information across social networks is necessary. There are intimidations in the use of and social networking software, though these are often not well known. In particular, the extent to which information passing between individuals using the sites as a conduit, and the extent to which these sites intrude into the corporate network model.

For the individual, the most effective solution remains education of the user to keep him/her alert to what may happen and the precautions which can be taken. We need to make people aware that the Internet is not, in reality, a private place. A well formulated awareness program is needed to inform the citizen of the advantages and of the risks of social networking sites, and to provide an overall awareness, particularly to the young and vulnerable, of the need to be cautious in what they do online. A solidification of statute designed to guard personal information is necessary, and also work to define and then to protect data proprietorship rights in a online environment. Social networking sites are not going to go away – we are at the beginning of a major change in the way the Internet is used in daily life - and social networking will develop and become more influential as a social force in society.

CONCLUSION

Internet privacy encompasses a wide variety of topics and subjects. It can be understood as privacy rights that an individual has online with respect to their data, and violations of the same that take place online. Given the dynamic nature of the online sphere, privacy

concerns and issues are rapidly changing. However, due to their currently "immature" state, as well as deficient security analysis and design, they suffer from serious security issues, the most important of which is probably the threats on user privacy. On the one hand, providers of social networking services want to collect as much information as possible about their subscribers, in order to exploit it and make a monetary profit out of it (for instance, using it for marketing and/or advertising purposes). On the other hand, the majority of the users is uninformed of the serious inferences some of their actions may have on their privacy, such as uncontrolled "tagging" or excessive uploading of personal digital photographs. Data mining techniques and privacy preserving mechanisms are in a perpetual arms race. However, in order to ensure user privacy in social networks, additional steps need to be taken. This anonymity as well as the freedom of inquiry has led to the propagation of this offence. Many developed nations have passed laws which deal specifically with the issue of online privacy and have made efforts to define this offence. Many countries in the world other than India have their own data protection laws as a separate discipline under which all the matter are dealt. They have well framed and established laws, exclusively for the data protection.

The privacy policy issues are far less well-developed in terms of, specifically, their legal character, not least to the extent that it is actually still unclear whether or not this is an area that should be covered by legal provisions as such. For example, should the law force Facebook and other OSN sites to improve upon or even simply clarify their privacy policies, and – if so – how could this be affected? Would a mere display of a clear notice on the behalf of the provider be sufficient in providing the users with this information? Also, and perhaps most controversially, is the question of whether or not the users actually care about this to any real extent? While the users and the Bloggers are 'rallying in support of copyright' in order to protect their work, as was discussed above, can it really be said that there is the same attachment to one's personal data? Is its 'gathering' and storage perceived as being a simple consequence of participation in OSN communities, a price that users are willing to pay for the privilege? If there were to exist some form of legal recourse for a complaint of this nature, would such a complaint be forthcoming?