Information Privacy concerns and Surveillance in Social Media

Radhika Belapurkar
L.L.M. in Law & Development
Azim Premji University

ABSTRACT:

Right to privacy is directly proportional to the protection of the dignity of the person. Article 21 of the Constitution of India protects the right to privacy as well as promotes the dignity of a person[1]. There are different approaches to privacy and the degree of privacy may vary from person to person. Daniel Solove argues that privacy can be classified into various categories which may often overlap and the categories are right to bodily privacy, right to be let alone, right to control over personal information, right to secrecy, right to access to self, etc.[2] Dignity is closely related to the concept of privacy and this personal right cannot be infringed upon. Information privacy is one of the classifications under the broad concept of privacy wherein the person has the right to control over personal information. The right to have a control upon personal information has various elements such as collection, storage and access to information with regard to the privacy practices. The user has the right to know how the personal information will be used when is acquired by other interested parties as well protect the data from unauthorized access. Information privacy is an inherent right of a person which upon the infringement affects the person's dignity.

I. INFORMATION PRIVACY AND CYBERSPACE

In the age of information technology, computers are continuously engaging themselves in the recording of data. Every transactions of the user which takes place on the cyberspace, leaves an electronic trace. These traces are powerful means to obtain the information about the user. The recording of data ranges from saving the documents or files to recording the internet activities of the user. These data form a unique identity of the computer. The data produced by the computer when connected to the internet is enormous as the computer keeps a record of the website visited, the ads being accessed to and the searches on the internet. The websites are informed about the software installed in the system as well as the features of the software and other such details. Privacy plays an important role in this digital world where information is publically available but the question remains how can information on a public platform be regulated?

With the change in technology, communication has become easier with the help of various social media platforms such as Facebook, Twitter, Instagram, Snapchat and other such platforms. While using these mediums of communication, individuals tend to submit a potential amount of personal information which are recorded by them. Apart from personal data, the communications which are undertaken across these mediums

[1]K.S. Puttaswamy and others v. Union of India, (2017)10 SCC 641.
[2]Daniel J. Solove, *Understanding Privacy*, Harvard University Press, (2008).

are also recorded. These recorded materials are not only stored but also transferred.

After the introduction of smartphones, the threat of storing and transferring personal information. The Smartphone is constantly keeping an account of the location while traveling to various places. The apps which are present in the Smartphone record and store data when the app is being used. The GPS system in the phone produces accurate location of the user[3]. It can be inferred that the technology around us is collecting and storing the data which is unknown to the users. While downloading the apps, using social media platforms as well as other such platforms; the consent of the user is always taken to access the gallery, messages and other such details.

Cyberspace is a virtual world with an abundance of information. The information is fed into this world very passing second and has kept the world connected with each other. It is easy to obtain various kinds of information within a single click. The information which is available online also includes personal data of the people who are involved in this virtual world. This poses a major concern to the right to information privacy as it is an inherent right of every person.

Paul M. Schwartz contends that there three potential threats to the invasion of information privacy and those threats are computer, Internet Service Provider and websites[4]. They play a very important role in the virtual world of cyberspace. The Computer is the medium between the user and the cyberspace. They are a potential threat because while deleting a file hides it from the view of the user but does not destroy it. If the computer falls into the hands of the wrong person, the data which was deleted can be retrieved by following simple commands from the software program. The computer further stores the internet activity and the software protocols that create files which store the information about the website visited.

There are cookies present on the websites which are the tags or blocks of data which the website sends to and store on the hard drive of the user of the computer upon visiting the website. When the user revisits the website, the browser automatically sends a copy of the cookie back to the website. The website identifies the user as a previous visitor and allows the site to match the details with the previous searches. The cookies contain detailed information on the user's pattern of online activities.

When a user is surfing on the cyberspace, every internet activity which is undertaken will be considered as personal information. The cookies which are placed on the website record the personal information which is in the form of internet activities. The company sets up cookies the website with the objective to gather personal data in order to sell the data to interested third parties.

[3]BruceSchneier,*Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. New York, N.Y: W.W. Norton & Company, 2015.
[4]Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 Vand. L. Rev. 1607 (1999).

Another potential threat to information privacy is the Internet Service Provider ("ISP"). They record highly sensitive data on the consumer's online behaviour as well as collect basic information about the client. They also purchase personal data from the marketing companies, thus creating a database. They have highly accurate data about the user who is using the services of the ISP. The ISP have basic details of the consumer when the individual signs up for an account with the ISP and in addition to that, the ISP track and keep a record of the user's internet activities. Gaining access to information through click stream data is another method used by the ISP to obtain information.

Websites collect personal information and majorly contribute to recording and storage of data. They collect data either with the help of cookies as well as filling the registration forms provided on the websites. The personal information available on the websites range from medical records, criminal records, telephone numbers, residential addresses and other bank related details. This makes the individual information vulnerable in the cyberspace.

II. COMMUNICATION PRIVACY AND THE STANDARD NORM FOLLOWED ON SOCIAL MEDIA

The communication privacy management theory explains the process of self-disclosure in both social and online platforms. It describes the ways in which the disclosure mechanisms manage the privacy boundaries of the users as well as disclosure of personal information[5]. When the individuals involve themselves in the voluntary disclosure of the personal information, the information transforms from being privately owned to co-owned. This makes the information vulnerable to threats of being exploited. The individuals need to create a boundary to determine the categories of information into public and private. This will help in allowing the individuals in careful disclosure of information as well as set an expectation on the co-ownership upon the disclosure. Privacy concerns come into place when the individuals fear how could their personal information which is shared on the social media could be used or exploited. Personal communication can be expropriated with the help of technology and surveillance of e-mails and social media activity.

The formal privacy norms of the organization contain the professional ethics, codes, norms, and policies to deal with any kind of personal information. These policies often contain how privacy will be regulated which includes privacy commitments, codes, privacy standards and so on. These are standard form contracts which are non-negotiable. Professional discretion and confidentiality are part of privacy standard that the users have some reasonable expectations with the agencies they share their information with. The social media platforms have

[5]AnithaChennamaneni and AakashTaneja, Communication Privacy Management and Self-Disclosure on Social Media - A Case of Facebook(Last visited on Nov 02, 2018, 2:00 P.M), https://pdfs.semanticscholar.org/9ef3/0b61775be10b973ac4f31d9b85bc2b4d4a22.pdf.

default privacy setting of an opt-out system which is problematic as the burden of responsibility shifts on the user. The opt-in approach should be used a standard norm in the privacy as it disallows any invasion of privacy unless the individual expressly agrees to share his information[6]. The principle of opt-out which is applied by the social media platforms implicitly allows invasion of privacy unless the user opts out. It is necessary for the standard norms of privacy to take into consideration the opt-in approach to enhance the security on the platform.

III. PRIVACY CONCERNS ON SOCIAL MEDIA

The internet is an interactive space which makes the mode of communication between people easier while keeping the privacy concerns on stake[7]. Social media are websites and applications that enable users to create content, interact and participate in social networking. Social media platforms are available on Smartphone as well as personal computers. These platforms develop on a routine basis and very frequently we have a new platform is launched or taken down. The speed of evolving of the social media is at a very high pace which is redefining the boundaries on the cyberspace. The interactions on the social media platform are interpersonal. In order to protect privacy over the internet, it is important to consider that what information is private and what is not and the aspects of privacy which the users are concerned about[8]. While the technology is growing, users are more open to sharing their personal information as well as being concerned about their right to privacy. The interactions on social media involve a lot of personal details unlike, the factual personal details which is the major concern on the e-commerce website. The complexities of defining and extending the scope of privacy are of a greater degree in the social media.

While signing up on various social media platforms and websites, it often observed that the privacy policy is ignored by the users. The privacy policies are worded in such a manner that these platforms do not get entangled into legal implications. The safeguards on various websites are low and users are prone to certain cyberspace violations including invasion of privacy.

The terms of service of Facebook which the user has to accept before signing up gives the right to the Facebook Incorporation to collect user's personal as well as demographic data. They can monitor and analyse human behaviour pattern[9]. The data on the basis of which the Facebook can monitor is provided by the user. The users

[6] Bernhard Debatin, Ethics, Privacy, and Self Restraint in Social Networking(Last visited on Nov 02, 2018, 2:30 P.M), http://www.lucs.lu.se/wp-content/uploads/2017/01/kkeg17_littsem-3_ethics-privacy-and-selfrestraint.pdf.

[7] Obar, J.A. and Wildman, S, *Social media definition and the governance challenge: An introduction to the special issue.* Telecommunications Policy, 39(9), 745-750 (2015).

[8] Nan Zhang, Chong Wang and Yan XU, *Privacy in Online Social Networks*(19th October 2018, 10:30 A.M.), http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.662.8584&rep=rep1&type=pdf,.

[9]Wilson, Robert & Gosling, Samuel & Graham, Lindsay, *A Review of Facebook Research in the Social Sciences,* 7 Perspectives on Psychological Science, 203-220 (2012).

wilfully upload their personal data and on the basis of this data, the user behaviour is monitored. The social media has the consent to access the data when the user puts up personal information, but the issue is what does the consent include. It is important to analyse whether the consent needs to be understood in its broader sense or in a narrower sense. This will be answered only by the privacy policies of the platform.

There are various privacy risks which exist on Facebook including unintentional disclosure of personal information, threat to damage reputation, unwanted intrusion in the cyberspace, harassment, use of personal data by interested third party which maybe in most cases non-state commercial entities and vulnerability to the risk of cybercrimes, which may cause enormous financial and reputational loss.

There is a burden of responsibility which is shared by both the user as well as the social media platform. The burden of responsibility shared by the user in the form of the amount and the substance of the personal information which is being given out on the platform which includes personal details, photos, preferences, and other such details. The responsibility on the social media platforms is the privacy security controls on the website or the application as well as reducing the amount of use of this platform by the advertisers. The social media platform has an incentive to earn profits in the exchange of the information stored by these websites and due to this, the security and access controls are weak.

It is required for the social media platform to obtain the consent of the user before using the user's profile for the purposes of marketing or advertising[10]. The consent is based on the opt-out basis which may not be very useful as the advertisers on the social media platform keep increasing very frequently and it is difficult for the user to keep track of the same. There are numerous advertising companies associated with the social media websites and many of them are unknown to the users, it is difficult for the users to know as well as keep track of those companies in order to choose the option of opt-out. The privacy of the users is at stake as there are many advertisers which are unknown to the users who may have access to their personal information.

When an individual signs various privacy agreements without reading the terms and conditions, it is called consent fatigue[11]. This further leads to diminished consent as it becomes nearly impossible for the user to understand privacy policies[12]. The social media websites have a standard form contract which iscomplicated for the users to understand the implications of the terms which are given in the contract. The user accepts all the terms and conditions without carefully reading them. The consent is given without having proper knowledge about the same.

[10]James Grimmelmann, Saving Facebook, 94 Iowa Law Review, p. 1137 (2009),
[11] Rahul Matthan, Beyond Consent – A New Paradigm for Data Protection, Takshashila Discussion Document, 2017-03.
[12]*Id.*

The consent model on the social media platforms does not provide adequate protection to the users. Every internet activity is recorded and tracked. The financial transaction of the users is recorded and are correlated with details such as location, gender, age and so on. This correlated data then compiled and from which they create a profile of the user. This profile gives them an impression about the likes, dislikes, and preferences of the user, thus giving insights about the personality. The user has no knowledge of the same.

Exposure of the personal information reduces the capacity to protect the reputation in the society. Harm to reputation is irreparable and preserving one's personal information is essential to protect any intended harm to the reputation. It is difficult to grow or change out of the image which is already present or created on the cyberspace. There is a digital baggage present from the past which is carried forward to the present.

There are many privacy concerns which are created due to technology. These concerns are a product of various factors which include lack of awareness of the users, the privacy policy of the social media platforms, interference from the third party entities to gather personal information for their benefit, etc. The legal framework has not progressed that to the extent that the privacy of the users is protected in the cyberspace.

IV. SURVEILLANCE THROUGH SOCIAL MEDIA: A PRIVACY CONCERN

Databases which contain personal information are created by the companies is used as a tool for surveillance. Surveillance is a much debated issue as the ethical and societal implications of social media is questioned in the context of state and commercial surveillance. Surveillance can take place through social media have various features. Firstly, the user's activity on the social media platform reflects upon the identity construction of the people. This is created on the basis of tagged images, comments, and other posts. Secondly, social media platforms are equipped to monitor the profiles created on their network. The surveillance can happen by making use of the personal information which is visible, accessible and searchable. Lastly, the surveillance of profiles that holds information from many different contexts is known as social media surveillance[13].

The internet is a global information space which is interconnected with nodes in the network. These nodes help in combining and collecting data from the global information space about individuals. Global surveillance takes place in this manner with help of interconnected nodes in the network. Social media platforms which contain various professional and personal profiles are visible and can be traced for the purpose of surveillance, where the links between different people are observed.

The surveillance is undertaken by commercial entities as well as state entities. The information processed by the commercial entities can lead to exploitation of the data by selling it to advertisers on the basis of user generated content. The state surveillance over social media is to keep a check on the views of the citizens

[13]Christian Fuchs, Social media surveillance (Last Visited Nov 1, 5:30 P.M.), http://fuchs.uti.at/wp-content/DS.pdf,.

especially with respect to the state. Government buys data from the surveillance companies. These surveillance companies buy data from the social media networks. The monitoring software used in social media network strack the location from where the posts are being uploaded apart from monitoring events, identifying relationships between people, etc. This data is used by the law enforcement agencies to track criminal and carry out other administrative functions[14].

Information privacy introduces the concept of obscurity in the social media platform. This idea is losing its importance in the cyberspace because of transparency as well as accessibility of information. Digitization of public records is one such instance where the question of lack of obscurity is dealt. It is noticed that a person's remote access to cyberspace is kept in the records. In this case, it can be concluded that no one can escape unrecognized in the internet space. One of the important features of social media platform is analysis of information. The social media platform makes personal information accessible and transparent. It further monitors the information and analyses it, in order to derive additional information.

The methods used for monitoring personal information from social media is very secretive. It is unknown to the users about the amount of data collected by them, contents of the data as well as the ambit of information collected by them. The function and nature of the algorithms used by them is also another aspect which the users are unaware about[15]. This is another side of the coin where users are left uninformed about various mechanisms about the information available, data accessibility, collection, processing, storage and usage. The regulatory mechanism in place is not very effective to resolve issues of social media surveillance. It is often observed that the government and the commercial entity have an understanding between them with respect to the social media monitoring. While having all these aspects in the background, it is noted that the information privacy of the person is always at stake.

V. LEGAL REGULATORY FRAMEWORK AND THE PRIVACY NORMS

In India, the recent case of K.S. Puttaswamy and others v. Union of India[16], discussed that the aspect of informational privacy in the terms of person's mind. It recognizes the control over the circulation of information which is personal to the individual. The infringement of right to information privacy takes place when such information is accessed and used in an unauthorized manner. Information privacy is a complex issue and they arise from the nature of information. The case further discusses that invasion of information privacy is difficult to detect as they can be invisible. Information can be accessed, stored and transferred without the knowledge of the individual. The debate with respect to information privacy in the case was delicate balances

[14]Jeramie D. Scott, *Social Media and Government Surveillance: The Case for Better Privacy Protections for Our Newest Public Space*, 12 J. Bus. & Tech. L. 151, 155 (2017).
[15]*Id* at 157.
[16](2017)10 SCC 641.

should be drawn between the permissible sphere of the state as well as the interest of the user in the protection of the privacy. There is no regulation in place for data protection to protect the right to information privacy. The court had recommended that legislation is required in order to protect and balance the interest of the state as well as the individual.

The privacy laws in the European Union are known as user-friendly laws. They include the mechanism of the opt-in approach. This approach gives the right to self-determination to the user as well as gives an option of consumer choice. While the laws in the U.S. favour the interest of the businesses do not provide for opt-in approaches.

The laws require pre-contractual information needs to be provided to the users. In the social media platform is necessary for the users to know how their personal information will be treated. This is done by the means of standard form contracts which have prejudicial terms. These contracts may be terms as unfair under the UK and EU laws since they indicate a significant imbalance of bargaining power wherein the burden of responsibility shifts on the user[17].

With the recent reforms in the European Union reforms in the General Data Protection Regulation(GDPR) there are changes which are suggested to the social media platforms in order to have high standards for privacy protection of the users. The individuals have the right to ask the organizations to delete their data under certain circumstances, without delay, wherein the organization has no legitimate interest in retaining the data. The framework provides for penalties if the data controller fails to act instantaneously. This is known as Right to be Forgotten[18]. Though there are many positive reforms in the framework but the process of review is beyond the articles prescribed.

VI. CONCLUSION

The level of surveillance and the growing privacy concerns on social media being undertaken undermines the rights which are protected in the Constitution as well as foundation principles upon which the democracy is based on. Personal information is publically available in the cyberspace and is being used for various purposes compels the individuals to reanalyse the concept of information privacy in public domain and the necessary regulatory mechanisms which are required in the present times. The public availability of information and the system of surveillance through social media is an important aspect which leads to invasion of the right to privacy. The threat of data being misused for inappropriate purposes and individuals failing to control their personal information is a major concern. There is a requirement for robust security mechanism in the form of a

[17] LILIAN EDWARDS, PRIVACY, LAW, CODE AND SOCIAL NETWORKING SITES (JANUARY 13, 2013),.

[18] SeyedEbrahimDorraji and Mantas Barcys, Privacy in Digital Age: Dead or Alive?! Regarding the New EU Data Protection Regulations (2014), https://www.mruni.eu/upload/iblock/b97/ST-14-4-2-05.pdf.

legal framework to protect the right to privacy. In addition to that, there is a requirement for adequate protection on social media platforms over the personal information of the users.