# PRIVACY THREATS AND ITS LEGAL PROTECTION ON SOCIAL NETWORKS

Dr. R. Varalakshmi

Assistant Professor
Department of Computer Application,
The TamilNadu Dr. Ambedkar Law University, India.

***Abstract:*** The term social networks can be given as “a community of individuals who can share a common information by connecting to each other via their social interest, and thus bonded together using social network sites”. Many of the sites are free and allows individuals to submit their personal, professional and family interest which are reachable to all the citizens. Moreover, individuals feel it as a status in having a social network admittance for themselves. Social network sites permit individuals to create a friend’s group wherein the individual profile data are posted in public. In that case, an individual should be aware of the privacy and security issues of social networks. The personal data of individuals could be misused by unauthorized users. In this paper, some of the common privacy issues in social networks are explained on the perspective of right to privacy, the legal protection on social networks in India.

***Index Terms* - Social networks, privacy, legal protection, Right to Privacy.**

## I. INTRODUCTION

With the development of social network and the growing population of users of online communication using social media, more sensitive and secret information about individuals are available online. The disclosure of publicly available secret data could lead to the disclosure of their privacy. The individual privacy is at more risk when it is publicly available, traced and these activities could be interconnected with the data mining and extracting secret information from it. Depending on situation, Privacy has various synonyms in context of contents that are shared. If individuals keep their privacy setting on their social media like Facebook account as public, the intruder can easily view all the information. Instead, if they set the customized privacy setting, then it could be accessible only be their friends. There exist various threats especially relevant to social networks.

According to the Article 12 of Universal Declaration on Human Rights, “No one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks”. Thus, privacy rights are respected and is meant for community welfare. Article 21 established in India says the right to privacy.

The right that someone violated has something to do with individual ownership of the computer and manipulated something without the owner’s permission. The importance is that, the transmission mode means in which data are gained, shared but also the nature of data is the pivotal factor to be considered. As per the policy rules of the social networks, the information’s are shared by the individuals voluntarily, and hence cannot claim for privacy violation. But undoubtedly when the information is shared by other individuals by way of hacking, fraud or any other method of cybercrime then one can claim that there exists privacy violation.

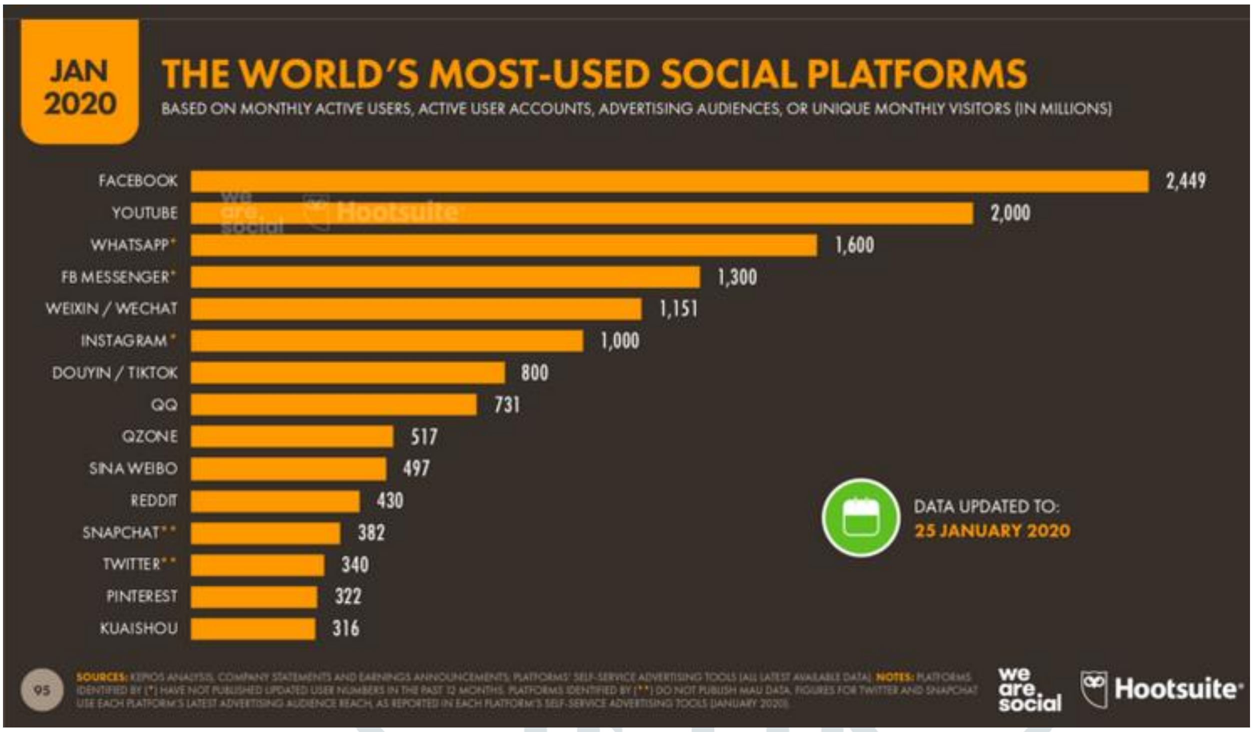
## II. PRIVACY IN SOCIAL NETWORKS

The individual privacy is at more risk when it is publicly available, traced and these activities could be interconnected with the data mining and extracting secret information from it. There are more than 3.8 billion users using social media or network throughout the world which represent 49% of the total world population. Out of all social media, Facebook ruins the world’s utmost extensively used social media platform. The total active individuals on various popular social media are presented in Table 1.

Table 1.1: Social media platforms now have 300 million or more Monthly Active Users (MAU)

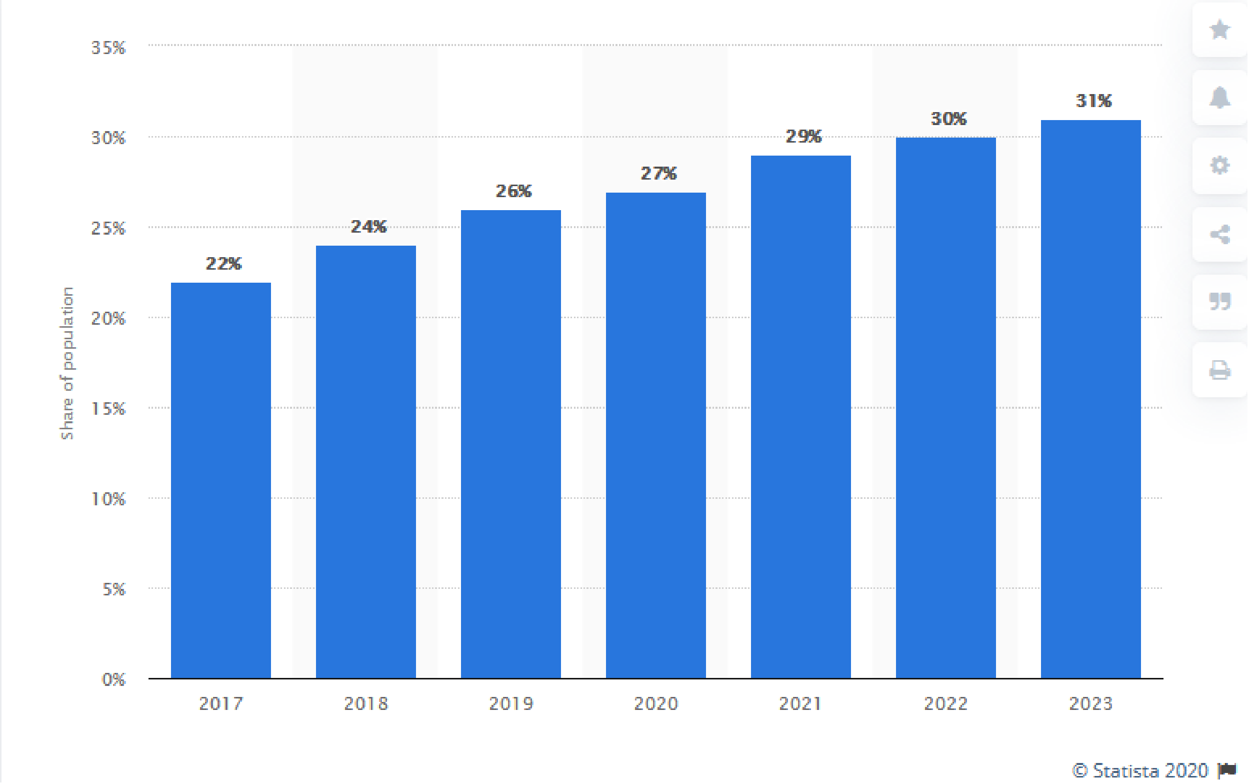
| Social media platforms | Monthly Active Users (MAU) |
|---|---|
| Facebook | 2.45 billion |
| YouTube | 2.00 billion |
| WhatsApp | 1.60 billion |
| Facebook Messenger | 1.30 billion |
| WeChat (Weixin) | 1.15 billion |
| Instagram | 1 billion |
| TikTok (Douyin) | 800 million |
| QQ | 731 million |
| QZone | 517 million |
| Sina Weibo | 497 million |
| Reddit | 430 million |
| Snapchat’s | 382 million |
| Twitter’ | 340 million |
| Kuaishou | 316 million |

Figure 1 illustrates the worlds most used social platforms.



Source: https://datareportal.com/social-media-users

In 2018, 24 % of India's population was accessing social networks. Figure 2 illustrates prediction that by 2023, this diffusion of social networks would be 31% of the country's population.



Source: https://www.statista.com/statistics/240960/share-of-indian-population-using-social-networks/

Figure 2: Percentage of population using Social network in India from 2017 to 2023 (forecast)

Table 1.2: Percentage of population using Social network in India from 2017 to 2023 (forecast)

| Year | Share of Population (%) |
|---|---|
| 2017 | 22 |
| 2018 | 24 |
| 2019 | 26 |
| 2020 | 27 |
| 2021 | 29 |
| 2022 | 30 |
| 2023 | 31 |

With the ease of internet access, the number of social media users in India stood at 326.1 million in 2018. Number of social network users in India from 2015 to 2018 with a forecast until 2023 (in millions).

Since the usage of social media are high, individuals could be exposed to privacy threats. The threats that are only related to social networks are listed. According to the report the social networks are not in risk assessment scoring system but it is considering as the top categories of platform for cybersecurity.

## III. Privacy Threats on social networks

This section deals with the threads especially relevant to social networks. If individuals keep their privacy setting on their social media like Facebook account as public, the intruder can easily view all the information. Instead, if they set the customized privacy setting, then it could be accessible only be their friends. So upon accepting the friend request from some unknown, the intruder uses this way to collect the individuals personal information from their peer group wherein the publicly available contents could be hacked by the intruder by employing inference attack.

### 3.1 Clickjacking attack

Clickjacking attacks is a user interface redress attack. In this attack, an intruder can manipulate the social network individuals into posting some spams and requests to unknown links. Here, an intruder can even try to monitor and record the activities of the hardware components of a computer used by an individual.

### 3.2 De-anonymization attack

De-anonymization is an attack where unidentified information that are sent are cross-reference with public. We know that social networks provide strong content or data sharing. In order to access these data without loss there are many deanonymization strategies to reidentify an individual information.

### 3.3 Fake Profiles attack

In this attack an intruder generates an account with fake IDs on social network and sends messages to genuine individuals. The aim of this attack is to collect the private information of individuals from the social networks which is available only to their friends, and spreads it as spam. It misuses the information, which gives misleading information to others.

### 3.4 Inference attack

This attack is employed to predict the private and complex information of individual that is kept secure. It predicts the attributes of an individual with other public attributes that exist online.

### 3.5 Cyberstalking

It is to harass an individual or group via internet or social networks. It is used for monitoring, identifying threats, gender etc.,

### 3.6 Surveillance

This a new type of monitoring called as social network surveillance. It monitors the different activities of their individuals in various roles by hacking their profiles and relationships with another person. This surveillance is used to monitor the human activities on social media which is of technology-based.

In general, the court of law and the violation of right to privacy are given as the solutions to solved any kind of problem. What makes this more complex is the transmission medium like internet, on which the information has been violated.

The following are some of the laws available in India which deals with the violation of right to privacy on social networks via internet.

- Constitution of India
- The Information Technology Act, 2000
- The Right to Information Act, 2005
- The Companies Act, 2013
- Mutual Legal Assistant Treaty

At eras it is requirement to rethink about the tactics for defining the violation of privacy taking place via online mode and then the protection route for securing right to privacy could be finalized.

The individual legally responsible for posting any convicting, illegal content via social media are made firmly to come under The Information Technology Act, 2000. The IT Act under sections 72 and 72A provides the punishment for both confidentiality breach and privacy violation. The cyberlaw of India is a legislation that covers multiple extents.

## IV. Conclusion

Social network or media have many rewards but rather than advantages, social networks have some issues related to privacy rights. Unauthorized access to information raises privacy issues that could occur from social network. In this paper, various privacy rights, threats and laws related to right to privacy were discussed. As right to privacy concept progress, the laws that assign liability for invasion of privacy remains. The main purpose is to instruct social network individuals on protecting themselves from privacy issues and also to make an individual aware of right to privacy.

## References

**[1]** Protalinski, E. 2018. Chinese Spies Used Fake Facebook Profile to Friend Nato Officials.

**[2]** Vishwanath, A. 2017. Getting phished on social media. Decis. Support Syst. 103, 70–81.

**[3]** Ashtari, S. 2013. I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy. J. Inf. Priv. Secur. 9, 80–82.

**[4]** Lundeen, R.; Ou, J.; Rhodes, T. 2018. New Ways Im Going to Hack Your Web APP. Black Hat AbuDhabi. Available online: https://www.blackhat.com/html/bh-ad-11/bh-ad-11-archives.html#Lundeen

**[5]** Gulyás, G.G.; Simon, B.; Imre, S. 2016. An Efficient and Robust Social Network De-anonymization Attack. In Proceedings of the Workshop on Privacy in the Electronic Society, Vienna, Austria, pp. 1–11.

**[6]** Perlroth, N. 2013. Fake Twitter Followers Become Multimillion-Dollar Business. The New York Times, Available online:https://bits.blogs.nytimes.com/2013/04/05/fake-twitter-followers-becomes-multimillion-dollar-business/?_php=true&_type=blogs&ref=technology&_r=0 (2018).

**[7]** Lewis, J. 2012, How spies used Facebook to Steal NATO Chief's Details. The Telegraph.

**[8]** Heatherly, R.; Kantarcioglu, M.; Thuraisingham, B. 2013. Preventing private information inference attacks on social networks. IEEE Trans. Knowl. Data Eng. 25, 1849–1862.

**[9]** Burke Winkelman, S.; Oomen-Early, J.; Walker, A.D.; Chu, L.; Yick-Flanagan, A. 2015. Exploring Cyber Harassment among Women Who Use Social Media. Univers. J. Public Health, 3, 194–201.

**[10]** Fuchs, C.; Trottier, D. 2015, Towards a theoretical model of social media surveillance in contemporary society. Commun. Eur. J. Commun. Res. 40, 113–135.

**[11]** Andrei Marmor. 2015. What Is The Right To Privacy?, Philosophy & Public Affairs, Wiley Periodicals, Inc 43,no. 1.

**[12]** Connie Davis Powell, 2013, Privacy for Social Networking, UALR Law Review, Vol 34, taken from http://ualr.edu/lawreview/files/2013/01/Powell-Normal.pdf .

**[13]** Mann, Bruce, 2008. International Journal of Law & Information Technology, Vol (2), 2008.