RIGHT TO PRIVACY AND THE LEGALITY OF SURVEILLANCE

Author: Shabnam Kausher, (Advocate) B.A. LL. B., LL.M.

Abstract

Digital communications technology like the Web, cellular phones, and Router devices are becoming commonplace. Telecommunications technical advances have increased the right to free speech, enabled global discussion, and promoted civic involvement by substantially expanding access to data through real-time interaction. These potent tools offer enhanced equal enjoyment of all humans by magnifying the perspectives of human liberties guards and equipping people with technological skills to record and uncover injustices. The Internet has developed both pervasive and more personal as modern life is progressively carried out on the internet. Significant worries have been voiced as laws and procedures in governments throughout the world that leverage the susceptibility of modern telecommunication technologies to video surveillance and intercept have indeed been uncovered. Subtle and overt internet monitoring have spread in countries throughout the globe, with official wiretapping becoming a hazardous practice instead of an unusual action. Authorities allegedly threatened to remove the facilities of telecommunications and network gear businesses if they were given clear access to social traffic, utilised fibre-optic wires for military surveillance, as well as required businesses to routinely disclose high volume data on employees and customers. As a result, the linked article has critically addressed, with referenced case examples, the Indian administration's legal involvement for data security and privacy problems inside the framework of the Personal Data Protection Bill, 2019, the 1974 Privacy Act, and also the Bureau of Indian Standards.

Key words*:* Privacy, Digital platform, protection, surveillance

Introduction

Since the appearance of early informal communication locales in the mid 2000s, online interpersonal interaction stages have extended dramatically, with the greatest names in web-based media during the 2010s being Facebook, Instagram, Twitter and Snapchat. The huge inundation of individual data that has opened up on the web and put away in the cloud has put client protection at the bleeding edge of conversation in regards to the data set's capacity to

securely store such close to home data (Watt, 2017). The degree to which clients and online media stage heads can get to client profiles has turned into another subject of moral thought, and the legitimateness, mindfulness, and limits of ensuing protection infringement are basic worries ahead of the mechanical age. Informal organisations have turned into a piece of human existence (Laidlaw, 2017). Beginning from sharing data like message, photographs, messages, many have begun share most recent news, and news related pictures in the Media area, question papers, tasks, and studios in Education space, online study, advertising, and focusing on clients in Business space, and jokes, music, and recordings in Entertainment space (Nyst, & Falchetta, 2017). As a result of its use by Internet surfers in every conceivable manner, even small would specify the long range informal communication media as the current Internet culture. While partaking in the data sharing on Social Medias, yet it requires an incredible arrangement for security and protection. The clients' data that are to be kept undisclosed, ought to be made private.

Social Media and Privacy

Protection concerns have by and by been at the centre of attention as of late after reports asserted that the Pegasus programming was being utilised to keep an eye on many individuals all around the world incorporating various in India (van Hoboken, 2019). The Supreme Court of India, while requesting an autonomous test into the claims, noticed that reconnaissance encroaches on the right to security of a person. Perhaps the main question introduced here was the place where a singular's all in all correct to protection lie in the bigger setting of public safety. Online media is presently considered as probably the greatest danger to individual security (Beigi, & Liu, 2018). Activities of web-based media goliaths as of late have featured these issues. Facebook's name in regards to the capacity of online media organisations to gather and abuse client information in the clothing of client assent despite the fact that no genuine decision has been given to clients (Lapenta, & Jørgensen, 2015).

Data Scraping

Third parties might scan and compile data supplied to publicly released social media, irrespective of the stipulation of the social sites and even technological precautions designed to restrict data harvesting.

Data scraping is a broad word that refers to a variety of Internet-based information retrieval methods which are utilised against the consent of the data holder (Zhao, 2017). Scraping information can indeed be done manually or automatically; when done electronically, machine-to-machine communication is employed. Data scraping is common in corporate activities. Even though it may not appear obvious, recruiting efforts, trend recognition, advertising campaigns, purchases and generate leads, line of credit and client hazard identification, and intel gathering practises all use data scraping to improve their database systems, sources of information, and specific functionality.

Fortunately for consumers, new rules such as GDPR as well as other proposed laws have rendered it more difficult for firms to acquire and store information with (or without) consent of the people (Sirisuriya, 2015). In certain circumstances, media platforms such As facebook and sometimes even Apple's App Store have significantly curtailed the volume of content third-party programmers may access via the platforms' APIs.

However, for firms whose activities depend on publically viewable data, the inaccessibility to that plethora of data has clearly harmed their profitability. To stay solvent and avoid new regulatory standards, some businesses have resorted to a tried-and-true technique of data collection: web scrape.

Facebook apps leaking personal data

Private details of over 533 million Facebook members spanning 106 countries were discovered to have been exposed earlier in the year (Symeonidis, et al., 2018). Alon Gal, CTO of cybersecurity company Hudson Rock, is the first one to warn in January that a Telegram bot would be used to trade contact information for gratis. The bot exploited a flaw in a Facebook function that enabled phone numbers associated with any profile to be accessible freely. The recent data breach is being linked to that problem, with Facebook

confirming that the information is two years old. It had also officially recognised the violation at the time.

In 2011, Facebook reached a settlement with the Federal Trade Commission on allegations that it failed to uphold its confidentiality guarantee to customers by enabling personal data to be made available to the public prior notification (Lovato, et al., 2020). According to authorities, Facebook erroneously claimed third-party applications could only obtain the information they required to function. In fact, the applications might gain entry to practically all of a subscriber's private details. If their friends utilised apps, Users of facebook who have never verified a third-party app may well have their personal postings captured. Facebook had also been accused of disclosing user data to marketers, despite promising not to.

Online social tracking

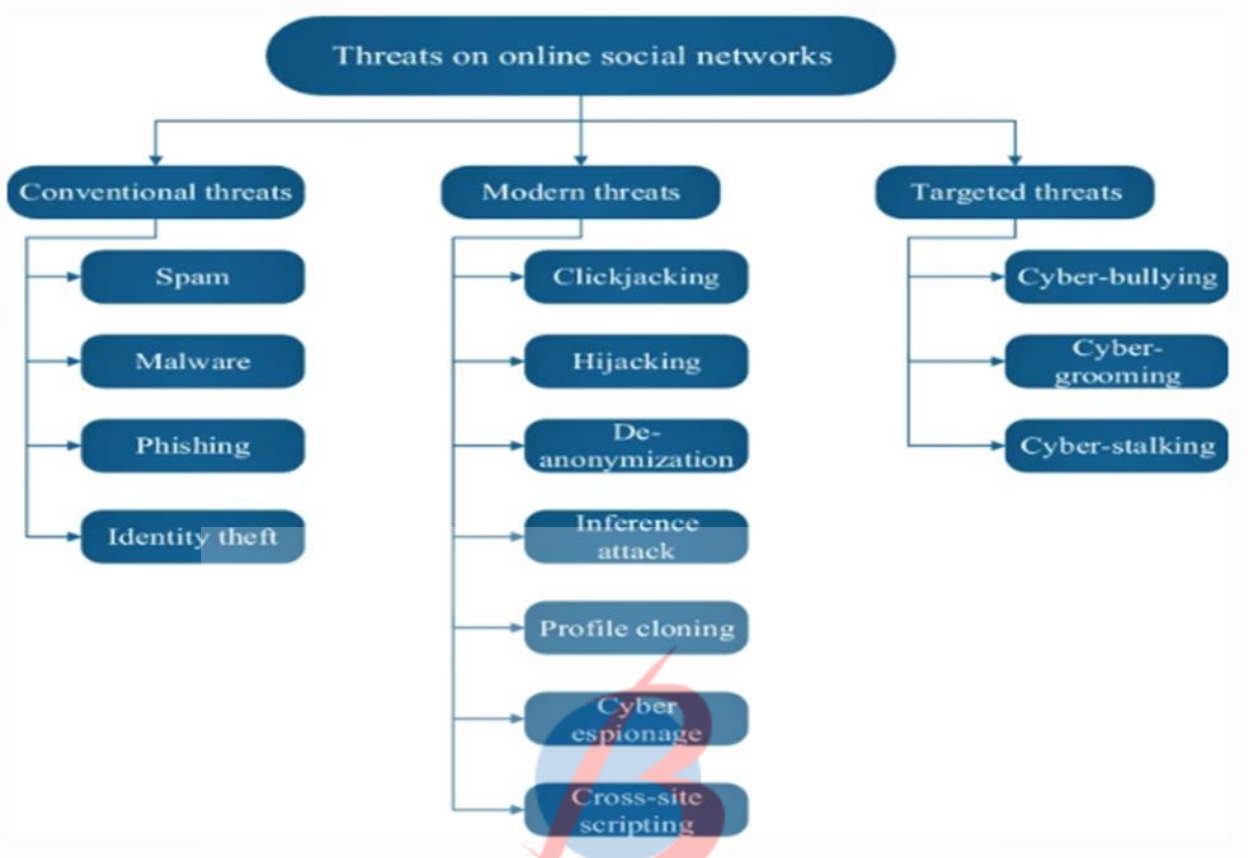
Online social networks (OSNs) have risen in importance in recent times of rapidly evolving technology (Shao, et al., 2016). The capacity of OSNs to offer a stage for customers to communicate with their relatives, colleagues, and professionals is the driving force underlying this phenomena. Data published on social networks and multimedia quickly spreads, nearly instantly, making it appealing for hackers to get intelligence. The confidentiality and security of OSNs must be investigated from multiple angles. There are many privacy and security concerns associated with the user's information shared, particularly when the user submits private information such as pictures, movies, and audio recordings. The hacker can utilise supplied data intentionally for nefarious objectives. When adolescents are approached, the dangers are multiplied (Castro, & Shaikh, 2018).

As per Heimdal Security, approximately 6 lakh Facebook pages are attacked everyday .Users who spend more hours on social networking and are therefore more likely to accept their group members' postings. This confidence is exploited by cybercriminals. Social networks may also be used by attackers to rig politics. Like-jacking, that happens when hackers upload bogus Facebook like icons to web browsers, phishing websites, and spam mails, is among the most common social networking assaults.

Causes of privacy exploitation

Online web-based media can present new dangers for their clients in light of the potential for getting to an immense measure of individual data revealed by OSN users themselves (Sbroiavacca, & Sbroiavacca, 2018). Various sorts of resources are inclined to assaults in OSNs, including private information of the people or associations, advanced character, financial assets, intellectual property (IP), and corporate privileged insights and resources. OSNs can be the objective of a few kinds of assaults like spamming, phishing, clickjacking, and cross-site prearranging, to give some examples.

The primary driver behind friendly designing assaults is the way that OSN clients are not mindful of the genuine worth and significance of private data and, as a result, they don't give a lot of consideration to protect it against assaults sent off by malicious users (Babalola, 2021). In such a circumstance, the aggressor can beguile clients into uncovering confidential information utilising distinctive mechanisms.A invert social designing assault is one more danger to OSNs in which themalicious assailant deludes the client into reaching him utilising various sorts of techniques. Since the client starts the association, a more significant level of trust is established between the assailant and the client. After this association is established with the deluded client, the assailant starts his malignant activities, for example, phishing and spamming (Sevignani, 2015).



Legal interventions

1974 Privacy Act

The Privacy Act of 1974 governs how an administration's record-keeping system is managed and how data is communicated with certain other government departments and people (Liv, & Woods, 2020). In February 2011, the Department of Homeland Security (DHS) issued a Network of Documents Notification detailing its surveillance of social networking sites in accordance with this statute. There are no severe constraints on data gathering as well as usage as long as a number of procedures defined in the rule is implemented. Federal and state eavesdropping laws set severe restrictions on state eavesdropping of phone conversations. While this restriction doesn't really immediately extend to anything put on social networking sites, it demonstrates how defensive the legislation may be when it comes to evaluating conversations that are considered private (Bennett, 2018).

Personal Data Protection Bill, 2019

A parliamentary committee has recommended major changes to the draught Personal Data Protection Bill for 2019. It proposed calling the law the Data Protection Bill, 2021, as well as expanding the scope of the law to encompass non-personal data directly in addition to the individual information (the Bill). The Bill proposed an integrated structure for information security as well as establishing a seven-member (along with the chairwoman) Data Protection Authority (DPA) (Fefer, 2019). While the government is an information custodian that has dispositional responsibility over the handling of the principal's private information, the government has been given extensive exceptions.

Bureau of Indian Standards

The Bureau of Indian Standards ("BIS") published general data protection security standardisation, known as IS 17428.1. It is meant to give a structure for enterprises to create, operate, administer, and constantly enhance their online privacy control system. It is a credential that allows firms to reassure their consumers and workers about their confidentiality procedures, and it may be tactically utilised to differentiate themselves from market rivals. The Bureau of Indian Standards (BIS) is a standards development authority in India that oversees standardisation, quality assurance, and performance measurement of products and services (Stewart, & Stewart, 2017).

Case study

Justice K.S. Puttaswamy v. Union of India

The Supreme Court of India issued its decision in the matter of People's Union for Civil Liberties (PUCL) against Union of India (SC, 1997), that established the privacy rights in the framework of telecommunication monitoring (i.e. wiretaps) with fundamental independence. This article analyzes the Supreme Court's attitude on anonymity in the PUCL Matter, which had been affirmed in the historic 2017 verdict by the nine-judge panel in KS Puttaswamy against Union of India (SC, 2017) that proclaimed confidentiality to be a constitutional right (Puttaswamy, 2017). The contextual relevance of the privacy rights in the frame of reference of wiretaps was additional sensors in the October 2019 judgement in Vinit Kumar vs Central

Bureau of Investigations and Ors (Bom HC, 2019), in which the Bombay High Court highlighted the scope of the government's ability to interrogate its areas of study, especially on things that matter who do not come under the umbrella of 'national emergency' or 'in the name of public safety.'

Moreover, there have already been judgements by narrower Supreme Court bar stools, like R. Rajagopal vs Union of India (SC, 1994) (Ramachandran, 2014)and Gobind Sharma versus Union of India (SC, 1975) wherein the privacy rights has already been managed to hold to be a protected by the constitution basic right, because it is in this context that perhaps the PUCL Instance possesses significance.

Conclusion

Online social networks have turned into a crucial piece of the huge web infiltrated world. The change in perspective has empowered informal organisations to draw in with clients consistently. The expanded pace of web-based media use has requested the need to make its clients mindful of the traps, dangers, assaults, and security issues in them. With the progression in innovation, online media has taken different structures. People can interface with one another in a bunch of ways. Subsequently, there is a convincing need to persistently and iteratively audit security issues in informal communities keeping in pace with innovative progression. In this paper, introduced various situations connected with online informal community dangers and their answers utilising various models, systems, and encryption procedures that secure the interpersonal organisation clients against different assaults. Generally speaking, analysts can assume a critical part in the guarded methodology against these assaults in OSNs yet at the same time, a few issues should be settled by utilising some half breed approach, system, and danger recognition devices.

References

1. Babalola, O. (2021). *The Impact of Privacy Issue and Data Exploitation in Achieving a Successful Mobile App* (Doctoral dissertation, Northcentral University). https://www.proquest.com/openview/b69820b44f0a3f1ee4119d0f1bbe1c98/1?pq-origsite=gscholar&cbl=18750&diss=y

2. Beigi, G., & Liu, H. (2018). Privacy in social media: Identification, mitigation and applications. *arXiv preprint arXiv:1808.02191*. https://arxiv.org/abs/1808.02191
3. Bennett, C. J. (2018). *Regulating privacy*. Cornell University Press. https://www.degruyter.com/document/doi/10.7591/9781501722134/html
4. Castro, L. E., & Shaikh, N. I. (2018). Influence estimation and opinion-tracking over online social networks. *International Journal of Business Analytics (IJBAN)*, *5*(4), 24-42. https://www.igi-global.com/article/influence-estimation-and-opinion-tracking-over-online-social-networks/212633
5. Fefer, R. F. (2019). Data flows, online privacy, and trade policy. *Congressional Research Service*. https://www.everycrsreport.com/files/20190311_R45584_caa16f89385a9b89430cfaac5d6633c392313c45.pdf
6. Laidlaw, E. B. (2017). Online shaming and the right to privacy. *Laws*, *6*(1), 3. https://www.mdpi.com/2075-471X/6/1/3
7. Lapenta, G. H., & Jørgensen, R. F. (2015). Youth, privacy and online media: Framing the right to privacy in public policy-making. *First Monday*. https://firstmonday.org/ojs/index.php/fm/article/view/5568/4373
8. Liv, T., & Woods, T. (2020). Privacy Act of 1974; System of Records. https://www.justice.gov/opcl/privacy-act-1974
9. Lovato, J., Allard, A., Harp, R., & Hébert-Dufresne, L. (2020). Distributed consent and its impact on privacy and observability in social networks. *arXiv preprint ArXiv:2006.16140*.https://arxiv.org/abs/2006.16140
10. Nyst, C., & Falchetta, T. (2017). The right to privacy in the digital age. *Journal of Human Rights Practice*, *9*(1), 104-118.https://epic.org/misc/The-right-to%20privacy-in-the-digital-age.pdf
11. Puttaswamy, J. K. (2017). v. Union of India. *Writ petition (Civil) No*, *494*.https://indiankanoon.org/doc/127517806/
12. Ramachandran, C. (2014). PUCL v. Union of India Revisited: Why India's Surveillance Law Must Be Redesigned for the Digital Age. NUJS L. Rev., 7, 105.http://nujslawreview.org/wp-content/uploads/2016/12/Chaitanya-Ramachandran.pdf
13. Sbroiavacca, A., & Sbroiavacca, F. (2018). INDUSTRY 4.0.: THE EXPLOITATION OF BIG DATA AND FORTHCOMING PERSPECTIVES. *Economic and Social*

Development: Book of Proceedings, 742-745.file:///C:/Users/user/Downloads/1038586.Book_of_Proceedings_esdLisbon2018_Online.pdf

14. Sevignani, S. (2015). *Privacy and capitalism in the age of social media*. Routledge.https://www.routledge.com/Privacy-and-Capitalism-in-the-Age-of-Social-Media/Sevignani/p/book/9781138940000
15. Shao, C., Ciampaglia, G. L., Flammini, A., & Menczer, F. (2016, April). Hoaxy: A platform for tracking online misinformation. In *Proceedings of the 25th international conference companion on world wide web* (pp. 745-750).https://dl.acm.org/doi/10.1145/2872518.2890098
16. Sirisuriya, D. S. (2015). A comparative study on web scraping.http://ir.kdu.ac.lk/bitstream/handle/345/1051/com-059.pdf?sequence=1&isAllowed=y
17. Stewart, D., & Stewart, D. R. (Eds.). (2017). *Social media and the law: A guidebook for communication students and professionals*. Taylor & Francis.https://www.routledge.com/Social-Media-and-the-Law-A-Guidebook-for-Communication-Students-and-Professionals/Stewart-Stewart/p/book/9781138695788
18. Symeonidis, I., Biczók, G., Shirazi, F., Pérez-Solà, C., Schroers, J., & Preneel, B. (2018). Collateral damage of Facebook third-party applications: a comprehensive study. *Computers & Security*, *77*, 179-208.https://eprint.iacr.org/2018/285.pdf
19. van Hoboken, J. (2019). 10 The Privacy Disconnect. *Human rights in the age of platforms*, 255.file:///C:/Users/user/Downloads/1005622.pdf
20. Watt, E. (2017). The right to privacy and the future of mass surveillance. *The International Journal of Human Rights*, *21*(7), 773-799.https://www.tandfonline.com/doi/abs/10.1080/13642987.2017.1298091
21. Zhao, B. (2017). Web scraping. *Encyclopedia of big data*, 1-3.https://www.researchgate.net/publication/317177787_Web_Scraping