Page 5733 - 5748 **DOI:** *https://doij.org/10.10000/IJLMH.111159*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 4 | Issue 3

2021

Personal Privacy on Social Media

NAYAN VARMA[1] AND ZUBA BUBERE[2]

ABSTRACT

With privacy just finding its tenets under the right to life and liberty, alongside it being accepted as a pivotal part of survival, every speculation regarding privacy; being online or offline is under scrutiny. Privacy means, holding and cradling the security of one's information, so that it is unsusceptible to unwanted viewers and its vulnerability remains unaffected in a cyber-attack. This abstract provides a brief overview of privacy as a concept intricately connected to an active social media user, the worry behind attributes that can affect the privacy of the user like data scrapping, leakage of personal data, social tracking, breach of data protection by social media giants and a comparative analysis of countries around the globe and their personal privacy laws. The subsequent article would also deal with an in-depth study on-Whether passwords ensure the privacy of information and personal security? Whether usage of location-based services is safe? Whether the layman is well informed before he participates on social media and whether programmers benefit due to misinformation of the general public mindset? Moreover, how is one to address the growing concern with respect to social media harassment including active and passive attacks in the light of an ineffective redressal mechanism? A revelation, pondering laymen come across is that, where exactly is privacy if not at home? when the same device used for logging into social media is allegedly suspected of catching personal verbal musings and overhearing conversations carried out in utmost privacy.

Keywords: *Privacy, Social Media, India.*

I. INTRODUCTION

Technological evolution has led to strange times, wherein information is being circulated continuously without any boundaries or limitations to adhere to. To the people, technology gives a perspective, not only does it showcase a ton of awaited information ready to access and breathe down, it even highlights how staying in touch with one another in a not so humane world is easily possible. But with the booming and blossoming world of technology, we fail to see risks arising from it. We fail to understand, how squarely and quickly can information

[1] Author is a student at Symbiosis Law School, Pune, India.
[2] Author is a student at Symbiosis Law School, Pune, India.

 [ISSN 2581-5369]

be compromised and fall in the hands of strangers. What happens to this information then? Documents of identity, health, finance, habits, activities, education and communication, photographs, video-clippings; all of this out in the open, ready to explore and divulge easily, privy to data mining, which leads to data being stored and leveraged to third parties without the user's consent. Fortunately, in a world post Edward Snowden, people are comparatively more aware of surveillance and diminishing privacy. Coming to establishing or rather reintroducing privacy, could be a difficult task because it hasn't been clearly defined nor have its ambits been precisely mentioned, and that's where the lacuna lies. A word unfettered and untapped can often be dangerous to combat.

The internet has been alleged to produce social media apps that detect your location, graphic images and content that have been compromised to threaten a person's personal privacy online. A revelation, pondering laymen come across is that, where exactly is privacy if not at home? When the same device used for logging into social media is allegedly suspected of catching personal verbal musings and overhearing conversations carried out in utmost privacy.

So, what exactly is privacy? An outlook of privacy was highlighted In R v. Edwards[3], a Canadian Supreme Court case, where Justice Cory helps in defining privacy as "*the state or condition of being alone, undisturbed, or free from public attention, as a matter of choice or right; freedom from interference or intrusion. An important aspect of privacy is the ability to exclude others from the premises. The right to be free from intrusion or interference is a key element of privacy.*" There are innumerable facets to privacy, and the one that needs utmost focus here is personal privacy because it's not a concept, it's a multi-dimensional world within itself. Justice Chelameshwar, while adopting Gary Bostwick's taxonomy of privacy, calls privacy *"an aggregation of rights, as it includes, the three interests of privacy of repose, privacy of sanctuary and privacy of intimate decision. Repose is the 'right to be let alone', sanctuary is the interest which prevents others from knowing, seeing and hearing thus keeping information within the private zone, and finally, privacy of intimate decision protects the freedom to act autonomously*". Thus, personal privacy inadvertently refers to holding and cradling the security of one's information, so that it is unsusceptible to unwanted viewers and its vulnerability remains unaffected in a cyber-attack or to simplify it a little, personal privacy is something one wants to preserve within themselves instead of letting it out in the open for the world to watch.

[3] R. v. Edwards, (1996) 1 SCR 128 (Canada).

 [ISSN 2581-5369]

II. UNDERSTANDING THE INCEPTION OF PRIVACY

The right to privacy was initially referred as a right by American jurists and this right flowed directly from the right to free speech, an important aspect of the first amendment of the United States book of law. Subsequently the Supreme Court of India, was awakened to the idea of privacy in the case of Kharak Singh v. State of Uttar Pradesh[4], wherein the petitioner complained of his right to privacy being violated by the police. Here close connections were sought to understand privacy with the concept of liberty. Liberty meaning to be free from unnecessary restrictions, free to live life in a manner one feels the need to, and free to keep things within oneself without the fear of leakage of this very information.

This was the starting point of privacy finding a footing in human rights with a reference to the European convention of human rights. Unfortunately, the cases of Kharak Singh along with M.P Sharma v. Satish Chandra[5], contained observations that privacy isn't protected by the Indian law at all. Several decisions like Gobind v. state of Madhya Pradesh[6], R. Rajagopal v. State of Tamil Nadu[7], People's Union for Civil Liberties v. Union Of India[8], Selvi v. State of Karnataka[9], Unique Identification Authority of India v. Central Bureau of Investigation[10]; explored dimensions of privacy after which the concept of privacy started being dealt with, amended and fine-tuned because the court was faced with a predicament regarding questions of interpretation of the constitution paying close attention to judicial discipline and integrity.

K.S Puttaswamy v. Union of India[11] held for the first time that right to privacy is protected as an intrinsic part and was thus implicit and flowing from the right to life and personal liberty, Article 21 of the Indian constitution and somewhere even Article 19 1(a), freedom of speech and expression. Moreover, the court stated that privacy wasn't an absolute right and it was subject to several restrictions by the state owing to the state's security and public interest.

The principle of proportionality was utilized to test infringements of privacy and this emanated from the European standard of proportionality, and is covered in the case of Modern Dental College & Research Centre vs. State of Madhya Pradesh[12], which stated that only those rights can be limited where the limitation is justified to protect public interest or the rights of people

[4] Kharak Singh v. State of Uttar Pradesh (1963) AIR SC 1295 (India).
[5] M.P Sharma v. Satish Chandra (1954) SCR 1077 (India).
[6] Govind v. State of Madhya Pradesh (1975) 2 SCC 148 (India).
[7] R. Rajagopal v. State of Tamil Nadu (1994) 6 SCC 632 (India).
[8] People's union for civil liberties v. Union of India (1997) 1 SCC 301 (India).
[9] Selvi v. State of Karnataka (2010) 7 SCC 263 (India).
[10] Unique Identification Authority of India v. Central Bureau of Investigation (2014) SLP CRL 2524 (India).
[11] K.S Puttaswamy v. Union of India (2017) 10 SCC 641 (India).
[12] Modern Dental College & Research Centre vs. State of Madhya Pradesh (2016) 7 SCC 353 (India).

 [ISSN 2581-5369]

at large. To put it pithily, if a limitation on a right is deemed constitutional then the law is proportional and if measures that are opted for in restricting the law but are for a particular purpose and the measures have a genuine connection with the purpose, then it is also considered proportional.

The Supreme Court thus has successfully managed to pave a way to hold privacy as a fundamental right while paying strict attention to infringement of personal privacy of an individual. Moreover, since privacy is still an evolving concept, it can be decided on case to case basis for further clarity.

Technological progress has resulted in a tense situation where the incompatibility between the right to privacy and data exposure is visually unbalanced so it's very important to understand the relationship between privacy and the social media user.

III. PRIVACY AND THE SOCIAL MEDIA USER

Justice Kaul in the Puttaswamy judgment identified concerns of surveillance and profiling, and he went ahead to emphasize on the impact of technology on the user, in the form of pervasive data generation, collection and its use in the digital economy. He also elucidates that the influence of this data can have an impact on actions of an individual which would result in a chilling effect, and its repercussions on free speech and expression. This recent judgment of 2018 re-establishes our doubts on the existence of a relationship between a social media user and social media itself. There's no denying that there is major influence of social media, be it on work performance, adolescents, children, relationships or any other kind of consumer. Social media distinguishes the sane from the insane and in a literal manner the cool from the uncool. It's a symbol of stature and pride for some and a big catalyst in terms of how a user lives its life. A social media platform is like a personal book of users details open to the view of all. It's a big diary of judgment. This diary is often compromised which results in data leakage.

We are living in an era where personal information can easily be utilized for various purposes like state surveillance and revenue generation for big businesses and phishing attacks are most often found on social media platforms wherein in 2019, a humongous phishing campaign was recorded targeting Instagram users by trying to pose as a two-factor authentication system leading to a false Instagram page. Highlighting this, the following words of Tim Cook, should be noted; "*Our own information is being weaponised against us with military efficiency. Every day, billions of dollars change hands and countless decisions are made on the basis of our likes and dislikes, our friends and families, our relationships and conversations, our wishes and*

fears, our hopes and dreams. These scraps of data, each one harmless enough on its own, are carefully assembled, synthesized, traded and sold."

The recent episode of Facebook failing to prevent Cambridge Analytica, related with Donald Trump's presidential campaign from gathering the data of 87 million users of Facebook to influence elections can also be taken to reflect on how easily personal information can be compromised thus resulting in privacy being a void space.

There are certain basic threats to privacy on social media which every user must be aware of while handling their data, which users consider as private and Malware sharing is ideally found on social media platforms as it is a conducive environment for malware distributors. What happens is that the malware infiltrates your computer and helps to steal sensitive information so that it can be misused. Botnet attacks are another common method to steal data and send spam which help cyber criminals gain access to devices and networks.

A data breach is due to the loopholes that give hackers the ease of breaking in and this was clearly demonstrated in the case where 422 million customers had their bank account numbers and balances leaked using the very bank's State Bank of India Quick Service. Moreover, there are databases sales on the dark net, where information was being sold easily. Location based services are also problematic in that aspect because recently an application Grindr came under the scanner for revealing the precise location of its users, according to investigations. Facebook and Twitter are often in the news where user's personal data is leaker by malicious apps because they have always undermined data privacy. The most infamous case is the Aadhaar case, which allegedly led to the leakage of personal data of Indian citizens for a menial price, clearly establishing the leakage hasn't been uncommon in the past years, which only points towards a stronger data protection act to be in place to monitor these very instances.

IV. THE INDIAN PRIVACY LAW REGULATING SOCIAL MEDIA

India has always lacked a privacy legislation until now when the Indian government is trying very hard to work and introduce the Personal Data Protection Bill 2019[13]. Nonetheless data protection was being achieved through other provisions like the Information Technology Act, 2000[14], The Indian Telegraph Act,1885[15] and Rules, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Rules) 2011, The code of

[13] Introduced in the Lok Sabha on Dec 11th,2019.
[14] Information Technology Act 2000 (No 21 of 2000 dated 17th Oct 2000).
[15] The Indian Telegraph Act,1885 (No 13 of 1885 dated 1st Oct 1885).

 [ISSN 2581-5369]

Criminal Procedure, 1973[16], The Unlawful Activities Prevention Act, 1967[17], Right to Information Act, 2005[18], The Indian Wireless Telegraphy Act, 1933[19].

India is now set out to have a comprehensive data protection law called the Personal Data Protection Bill, 2019 (PDP Bill), which provides for protection of personal data of individuals, and establishes a Data Protection Authority for the same. The Bill is the umbrella statute which protects personal data of individuals in India and processing of the same by the government, Indian companies as well as foreign companies.

The Bill defines personal data as *"data which pertains to characteristics, traits or attributes of identity, which can be used to identify an individual"* and this Bill differentiates data into personal and sensitive personal data and this encapsulates financial, biometric, caste, religious or political beliefs, or any other category of data specified by the government, in consultation with the Authority and the concerned sectoral regulator which would be subject to a heightened level of protection and safeguards.

Moreover, the Bill includes social media intermediaries[20] which provide a voluntary user verification mechanism for users in India resulting in the fact that intermediaries won't be able to share data or process it without intimation of the data principal. India is the only country that has the provision for a voluntary verification mechanism of this nature but there is prevailing ambiguity as to what proof the users need to submit to the social media intermediary to verify their accounts. But according to Srikrishna Bill, Section 40 of the PDP Bill has been done away with, meaning that companies like Facebook and Twitter would be able to store data of Indian users abroad if they so wish but only critical and personal data can be stored as data localisation has been toned down. The proposed Bill also deals with micro-targeting[21] as to mitigate any future incidents of political parties using data to micro-target voters, like in the case of Cambridge Analytica.

Reiterating aspects of the Bill that includes users' rights:

(i) obtain confirmation from the fiduciary[22] on whether their personal data has been processed,

[16] The code of Criminal Procedure (Act No 2 of 1974 dated 25th Jan 1974).
[17] The Unlawful Activities Prevention Act, 1967 (Act no 37 of 1967 dated 30th Dec 1967).
[18] Right to Information Act, 2005 (No. 22 of 2005 dated 15th May 2005).
[19] The Indian Wireless Telegraphy Act, 1933 (Act no 17 of 1933 dated 11th Sep 1933).
[20] 'Social media intermediaries' mean "entities whose primary purpose is enabling online interaction among users and does not include intermediaries that enable business transactions or access to the internet, or that are in the nature of search engines or encyclopedias".
[21] 'Micro Targeting' means "a form of online targeted advertising which analyses personal data to identify the interests of a specific audience or individual in order to influence their actions".
[22] A 'data fiduciary' means "any person, including the State, a company, any juristic entity or any individual who

(ii) seek correction of inaccurate, incomplete, or out-of-date personal data,

(iii) have personal data transferred to any other data fiduciary in certain circumstances, and

(iv) restrict continuing disclosure of their personal data by a fiduciary, if it is no longer necessary or consent is withdrawn. The Bill allows processing of data by fiduciaries only if consent is provided by the individual or in other cases where consent isn't provided it can be received by state on ground of emergencies.

The requirement that the government has an ultimate right to seek access to user's data and share non personal data could be concerning but the fact that auditors would be required to evaluate social media intermediaries for proper implementation is appropriate. Even though the Bill talks about informed consent that processes data in a fair and reasonable manner which respects the privacy of the individual it does not actually specify what constitutes as fair and reasonable which definitely needs to be addressed. This only makes it certain that social media companies would have to adhere properly to these regulations and requests, which otherwise would lead to a redressal procedure.

In comparison to Indian privacy laws, we also have a global presence of privacy laws with a wide range of regulations, which are one of few new and upcoming ones. The General Data Protection Regulation[23] is one such golden standard among data privacy regulations, which deal with employing data protection officers to organize personal data processing, stronger consent requirements, including biometric data, in the definition of sensitive data and enabling Data Protection Assessments. In terms of privacy protection both the PDP Bill and the GDPR are fairly similar albeit a few differences.

V. RESEARCH QUESTIONS

1. Whether passwords confirm the privacy of information and personal security?
2. Whether usage of location-based services is safe?
3. Whether the layman is well informed before he participates on social media and whether programmers benefit due to misinformation of the general public mindset?
4. Moreover, how is one to address the growing concern with respect to social media harassment including active and passive attacks in the light of an ineffective redressal mechanism?

alone or in conjunction with others determines the purpose and means of processing of personal data".

[23] European Parliament and Council of European Union (2016) Regulation (EU) 2016/679.

VI. WHETHER PASSWORDS ENSURE THE PRIVACY OF INFORMATION AND PERSONAL SECURITY?

Passwords are considered as one of the universally recognized and safest means of ensuring privacy of information and personal security. Log in through passwords is an extremely common practice in the present era. However, they are just like different keys to open the same door. This simply means that multiple persons can gain access to the same platform by logging in through the password set up by them. Given the ever-evolving nature of technology, sharing information among multiple devices has become a common phenomenon which in turn can pose serious risks. With the soaring number of cybercrime cases and an escalation in the gravity of the related crimes, passwords have proven to remain as a not-very-convincing safety code. Especially in cases where people set easy passwords for instance, date of birth, intruders find it extremely convenient to pounce upon access and control of an electronic device. However, setting up of a strong and unusual password is not an impossibility.

(A) Recommendations

Points to kept in mind while setting up Passwords:

1. **Do's and Don'ts:** There must be a list of do's and don'ts to be looked into before setting up a password.
2. **Passwords must be long and complex:** There must be a minimum of 8 characters; inclusive of uppercase and lowercase alphabets, numbers, special characters in order to ensure its strength.
3. **The auto-save option of saving passwords must always remain switched off.**
4. **Logging in on different devices:** When a particular portal is logged into using a password, it must be re-set in order to ensure that it is not stolen by anyone else post logging out.
5. **Shorter span for time-out:** Time-out should occur for not more than 5 minutes. The system must mandate a re-enter requirement in case of no-activity during the said period. This will reduce the possibility of any attempt to log in a personal account by a non-account holder.
6. **Personal computer security:** A personal computer must be secured with an authentic antivirus programme and other security checks in order to keep foreign elements at bay.

 [ISSN 2581-5369]

VII. WHETHER THE USAGE OF LOCATION-BASED SERVICES IS SAFE?

The disadvantages of usage of location-based services far outweighs its potential benefits. Some of the dangers may be analysed as follows:

- **Misuse of personal information without consent of users:** This is perhaps one of the scariest outcomes of misuse of location-based services facility. A good number of social media networks capture real-time location of its users. Such data is, at times, used as public information or as an update that can be viewed by authorized contacts.
- **Hacking and Tracking to cause physical injury/damage:** Using location-based services can be frightening by reasons of hacking too. If an application which tracks location gets hacked, all the movements of the respective person can get hacked. The safety and security of the person can be seriously prejudiced. Professional criminals and habitual offenders may engage in threatening, blackmailing and even raiding of houses and bank accounts with relatively less/ no practical remedy left to the victim.
- **Loss of data and confidentiality:** All the data that is stored on the device can be attacked. Such data can not only be used maliciously but also sold to third parties and perhaps result in huge losses. Therefore, location-based services can thrive upon the confidentiality aspect of business. There have been numerous petitions filed in the courts of law on the said and related grounds.

(A) Recommendations

1. The law must mandate an efficient and orderly due diligence to be undertaken in designing Location-Based Services by business entities.
2. Service Providers must be made accountable for greater transparency with users about Location-Based Services.
3. There must be some flexibility in obtaining consent of consumers. It has to compulsorily be an informed consent.
4. Understanding the Privacy Settings:

For Instance:

Facebook provides an option to turn off the new service by following these instructions:

i. Go to the Account tab and choose “Privacy Settings” (top right of Facebook page).

ii. Click “Customize settings” in the “Sharing on Facebook” section. (bottom left)

iii. Under “Things I share”, click the option box next to “Include me in ‘People Here Now’ after I check in.”

 [ISSN 2581-5369]

In order to block others from tagging you with the new location service:

i. Go to the Account tab and choose "Privacy Settings"

ii. Click "Customize settings" in the "Sharing on Facebook" section.

iii. Under "Things others share," click on "Friends can check me into Places."

iv. Click "Disable" from the list of options.

VIII. WHETHER THE LAYMAN IS WELL INFORMED BEFORE HE PARTICIPATES ON SOCIAL MEDIA AND WHETHER PROGRAMMERS BENEFIT DUE TO MISINFORMATION OF THE GENERAL PUBLIC MINDSET?

A high percentage of social media users lack basic understanding of the concepts of privacy and security. Privacy and security on social media platforms are greatly ignored unwittingly. This gives programmers a strong ground to benefit from the scenario and hence, encourages fraudulent activities. The perceived convenience of social media networks coupled with lack of privacy and security awareness have significantly contributed towards some of the major privacy violations.

Absence/ deficiency of social media education and awareness poses serious risks. In a state wherein programmers clearly understand the mindset of the general public, they manage to derive undue advantage and pounce upon such uninformed laymen in the areas of privacy, confidence, disclosure, defamation, intellectual property rights etc. including harassment and distribution of offensive material.

(A) Recommendations

1. Social media users must not feel obligated to participate on all kinds of social media platforms; especially the ones they are unfamiliar with.
2. Education regarding legal risks exposed though social media should be part of fully integrated school curriculum.

IX. HOW IS ONE TO ADDRESS THE GROWING CONCERN WITH RESPECT TO SOCIAL MEDIA HARASSMENT INCLUDING ACTIVE AND PASSIVE ATTACKS IN THE LIGHT OF AN INEFFECTIVE REDRESSAL MECHANISM?

According to a report by The Hindu, eight out of ten people have once in their lifetime experienced online harassment while over 41% of women have encountered sexual harassment in cyberspace.

 [ISSN 2581-5369]

1. Modes/Forms of Social Media Harassment

The Information Technology Act, 2000, (IT Act) expresses online harassment as an umbrella term to describe the use of the internet to harass, threaten or maliciously embarrass another party. It may take the form of verbal, sexual, emotional, or social abuse and aimed at a person, a group of persons, or even an organization. Cyber harassment, cyber abuse, online abuse are synonymous to the term "social media harassment".

There are innumerable forms of social media harassment. To name a few:

- Annoyance: for instance: rude comments made by online trolls
- Invasion: for instance: doxing
- Traumatization: for instance: cyberstalking and threats of violence

One mode of online harassment includes Email harassment. Email harassment incolves activities such as fake email IDs created with the intention to bully, threaten, blackmail, cheat or commit financial frauds on the victim. These email Ids are often offensive in nature.

2. Misuse of social media information and Privacy Policy

A lot of social media harassment revolves around online profiles and shared content. Profile information such as gender, birth date, place of residence, educational/workplace details is used to blackmail and threaten the account-holder. Sharing of content such as photographs have time and again stood as reasons for grave social media harassment.

A user may switch his privacy settings to the "Private Mode". However, certain information always remains publicly available. For instance: the username. No matter whether one chooses the Public or Private Mode for maintaining his/her social media account, he/she does not have the choice to restrict access to basic information such as the User Id. Moreover, social media networks are always in a position to modify their privacy policy without the approval of its subscribers. This simply means that the content which one posted considering that it is private and restricted it to be viewed only by the approved followers and friends, can now become visible to others. Privacy policies are able to cover social network only. Those third-party applications that interact with the website do not fall within its ambit. No social media network extends 100 percent guarantee for securing information on behalf of its users and so this can be looked upon as an obvious and well accepted ground negating the safety of participating on social media platforms.

3. Third Party Applications

For the purpose of interacting on social media networks, third party applications can do so

 [ISSN 2581-5369]

without actually being a part of the social network. The most common instances of such third-party applications comprise of online games. When one grants permission to such applications, social media networks share public information of its users with them. At times, certain private information may also be shared. Such third-party applications cannot be guaranteed as secure and may attack the user's device.

(A) Recommendations

1. Using a password manager to generate a strong password and for its assured storage.
2. In case of choosing security questions for password retrievals, inserting such questions the answers of which almost no one would know of.
3. A new Email address may be generated to link to social media accounts for added security of important data.
4. Review of privacy policy and the offered terms of service of social media networks periodically.
5. Restricting the provision/ sharing of personal information to the minimum.
6. Usage of third-party applications must be avoided as far as possible. In any case of non-avoidance, the terms and conditions of service laid down by such third-party applications must be carefully comprehended.
7. It is extremely important to log out from social media applications when not in use.
8. Connection requests from strangers must be rejected for the good. In any case where such stranger requests are accepted, then settings may be modified to choose as to what content of information shall be appropriate and willing to be shared.

X. Conclusion

Given the rampant increase in the magnitude of cases revolving around the subject matter as also the emerging complex nature and grave intensity of such crimes, there is an instantaneous need to address these issues directly. The Government must promptly intervene to not only come up with stricter laws but also ensure its implementation. It must also provide a strong corruption resistant mechanism for adjudicating disputes and lay down heavy compensatory norms, both on part of the grievance redressal machinery as well as the alleged offenders to be complied with in matters of breach. Such compensatory norms must far outweigh the cost of privacy investment in order to ensure compliance with the requirements.

The situation would eventually sort itself once contours of protections are laid down and the PDP bill is operationalized. It would be wrong not to take a moment to appreciate the herculean task of the government along with its participants to formulate such a robust framework.

 [ISSN 2581-5369]

Privacy is a sensitive topic which hasn't been dealt with progressively over the past many years, resulting in users either facing a backlash or receiving misinformation regarding the same. The acts infringing data privacy restrengthen the proposition that *a domesticated dog also bites* and what one considers a boon occasionally could also tip the scales heavily. This also calls for attention to the typical user behaviour whereby consumers unwittingly agree to submit their personal details on social media apps for usage of their services, which needs to carefully considered now, along with awareness to ensure the same.

*****

 [ISSN 2581-5369]

XI. REFERENCES

1. Aadhaar: Leak in world's biggest database worries Indians, https://www.bbc.com/news/world-asia-india.
2. Alysa Zeltzer Hutnik, Location-based Services: Why Privacy "Do's and Don't's" Matter, 20 iapp (March 8, 2012), https://iapp.org/news/a/2012-03-08-location-based-services-why-privacy-dos-and-donts-matter/.
3. An analysis of Puttaswamy: The SC privacy verdict, https://medium.com/indrastra/an-analysis-of-puttaswamy-the-supreme-courts-privacy-verdict-.
4. Anubhuti Matta, Know Your Rights: Online Harassment, The Swaddle (Feb 14, 2020), https://theswaddle.com/know-your-rights-protection-against-online-harassment/.
5. Anurag Vaishnav, "*The Personal Data Protection Bill, 2019: All you need to know*", https://www.prsindia.org/theprsblog/personal-data-protection-bill-2019-all-you-need-know.
6. Biggest data leaks of 2019, https://economictimes.indiatimes.com/industry/tech/8-biggest-data-leaks-of-2019-that-hit-indian-users-hard/information-of-100-mn-justdial-users-on-unprotected-server/slideshow/72837246.cms.
7. David Kessler, Sue Ross, Elonnai Hickok; A comparative analysis of Indian privacy law and the APEC cross-border privacy rules, (2014) http://docs.manupatra.in /newsline/articles/Upload/E6D7E8BE-1A25-440F-AEE0-66A5495A91D6.pdf.
8. Defining "Online Harassment": A Glossary of The Terms, Pen America, https://onlineharassmentfieldmanual.pen.org/defining-online-harassment-a-glossary-of-terms/.
9. Erica Jones, don't be caught short by lack of social media awareness, Maxim (Jan 2015), https://www.maxim-pr.co.uk/news/dont-be-caught-short-by-a-lack-of-social-media-awareness.
10. Haosheng Huang, Georg Gartner, Jukka M. Krisp, Martin Raubal and Nico Van De Weghe, Location based services: ongoing evolution and research agenda, Taylor and Francis Online, https://www.tandfonline.com/doi/full/10.1080/17489725.2018.1508763.
11. India's privacy bill will alter how it regulates social media platforms, not all of it good, https://thewire.in/tech/indias-privacy-bill-regulates-social-media-platforms.
12. Key Global Takeaways from India's Revised Personal Data Protection Bill, 2020, https://www.lawfareblog.com/key-global-takeaways-indias-revised-personal-data-protection-bill.

13. Key social media privacy issues for 2020, https://sopa.tulane.edu/blog/key-social-media-privacy-issues-2020.

14. Lack of awareness of social media risks, Monash University (Mar 21, 2011), https://www.monash.edu/news/articles/a-lack-of-awareness-of-social-media-risks.

15. PDP Bill 2019, https://www.prsindia.org/billtrack/personal-data-protection-bill-2019.

16. Personal Data Protection Bill, 2019.

17. Personal Data Protection Bill, 2019 –Examined through the Prism of Fundamental Right to Privacy – A Critical Study https://www.scconline.com/blog/post/2020/05/22/personal-data-protection-bill-2019-examined-through-the-prism-of-fundamental-right-to-privacy-a-critical-study/.

18. Personal data protection Bill 2019, looking at social media intermediaries and significant data fiduciaries, https://www.medianama.com/2020/01/223-pdp-bill-2019-social-media-significant-data-fiduciaries/.

19. Simplilearn, Understanding the Impacts of Social Media: Pros and Cons, Simplilearn (Sept 22, 2020), https://www.simplilearn.com/real-impact-social-media-article.

20. Social Networking Privacy: How to be Safe Secure and Social, Privacy Rights Clearing House (March 25, 2019), https://privacyrights.org/consumer-guides/social-networking-privacy-how-be-safe-secure-and-social.

21. S. Srinivasan, Lack of Privacy Awareness in Social Networks, ISACA (Nov 1, 2012), https://www.isaca.org/resources/isaca-journal/past-issues/2012/lack-of-privacy-awareness-in-social-networks.

22. Stefan Tanese, Location-Based Services Raises Privacy, Security Risks, Threatpost (August 25, 2010, 1.43 p.m.), https://threatpost.com/location-based-services-raise-privacy-security-risks-082510/74380/.

23. The Importance of Strong Secure Passwords, Security Data Recovery, https://www.securedatarecovery.com/resources/the-importance-of-strong-secure-passwords.

24. Tim Cook: Personal data collection is being 'weaponized against us with military efficiency', (2018), https://www.cnbc.com/2018/10/24/apples-tim-cook-warns-silicon-valley-it-would-be-destructive-to-block-strong-privacy-laws.html.

25. Tim Dwyer, Privacy from Your Mobile Devices? Algorithmic Accountability, Surveillance Capitalism, and the Accumulation of Personal Data (2020).

 [ISSN 2581-5369]

26. What India's privacy bill requires from social media firms (2019), https://www.outlookindia.com/newsscroll/what-indias-privacy-bill-requires-from-social-media-firms/1683099.

27. Xinyue Ye, Bo Zhao, Thien Huu Nguyen, Shaohua Wang, Social Media and Social Awareness, Springer Link (Nov 20, 2019), https://link.springer.com/chapter/10.1007/978-981-32-9915-3_12.

*****

 [ISSN 2581-5369]