VOLUME 4 | ISSUE 4

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

RIGHT TO PRIVACY VIS-A-VIS SOCIAL MEDIA

- Ayushi Saini[1]

INTRODUCTION

"In a world where everyone shows and tells everything,I value discretion and privacy"

Social Media Networks (SMNs) are one of the important evolutions that have happened in past decades. Some of the popular SMNs are Facebook, Twitter, LinkedIn, Snapchat, etc. Its speed and scope means that once content is posted it is available instantly around the globe. Social media is useful and used by all professions and ages. People of all ages and occupations use social media because it is helpful. Social media is radically altering not just how we interact with friends but also how we work by enabling connections between strangers, professionals, and friends that were previously unthinkable on a global scale. Privacy problems inevitably surface whenever personally identifiable information is exchanged and retained. As a result, protecting an individual's privacy in a domain like SMNs that is meant for sharing is challenging.

Social media affects the user privacy as it can control the information filled by the user, posts shared by user and other personal disclosures made by users publicalLy on these social networking sites. Additionally, social media networks can sync with applications on tablets and phones. Despite privacy regulations raising concerns, social media networks are trusted to protect user information by using these apps that request additional contact information from users. Sensitive data leaks may lead to legal action, consumer mistrust, brand harm, erosion of privacy, income loss, etc. Edited images and videos from user profiles can be used to threaten,

[1] Student at Amity Law School, Noida

blackmail, and defame specific users. Likes on postings and the interests of others can lead to contentious viewpoints and indicate a lot about a person.

The basis of privacy in western world was derived from the ancient political and civilized systems during the period of the Greek and Roman governments. Why is the political system so important as the source of the evolution of privacy in modern liberal society?

No matter how far humanity has come or when it first appeared, there has always been a need for privacy. In ancient India, the concept of privacy was integrated with the term "Avarana," meditation, and the Vedas and Upanishads. It also became a part of the concept of "Dharma." The Hindu and Muslim eras in India's history of privacy each have their own set of laws and customs thatseclusion. In India, the idea of privacy has long existed. It was ingrained in Indian culture's richlegacy customs.

With the improvements and popularity of social media, cyber crimes are rapidly increasing. Itis important to give attention to the issues and make strict rules and regulations with the dynamic technology. Individual users are very much interested in social networking sites like Whatsapp, facebook, etc especially women and children who are interacting with strangers onthese sites and meeting them which has increased the scope of crimes through social media. Proper attention should be given by the appropriate authorities in this matter.

RIGHT TO PRIVACY: NATIONAL LEGAL FRAMEWORK OF UNITED STATES OF AMERICA, UNITED KINGDOM AND INDIA

Man thinks that, the Right to Privacy is a special characteristic of human beings and the desire for privacy is a human function for the unique ethical, intellectual and artistic needs. But, the social scientists engaged in animal studies i.e. Prof. Alan F. Westin in disapproves that thinking. The Origin of Human Right to Privacy lies in the origin of man, i.e. in the animal world. Hence, discussion of man's patterns of privacy should be started chronologically from the man's evolutionary heritage. Though the origin of privacy is found in the animal society, but it gradually has been adopted by human society. The origin, history an development of Privacy can be summed-up as: The term 'Privacy' is derived from the Latin word 'privatus' which means separated from the rest. Though it is a variable concept and varies with cultural or social

context, but actually it means, the right to be left alone. The need for Privacy is to create a balance between individual and social interests, which is equally applicable to past, present and future society. In this sense, the necessity of Privacy was found in the dawn of human civilization. The idea of Privacy is as old as Biblical periods. Also the growth and expansion of Privacy varied according to the variation in different stages of human civilization. Hence, the description of origin and history of Right to Privacy should proceed from the ancient period to the modern period. In fact, the idea of Privacy was originated in the animal society and gradually it has been incorporated into the human society. The idea of Privacy, which was originated in the animal society, has been adopted in the primitive human society, where the traces of it were first found. According to different Anthropological studies, the idea of Privacy varied in respect of different primitive societies. With the evolution of primitive society to ancient society and then gradually to modern society, the idea of Privacy has been developed to get its present shape. The root of Privacy and its protection is embedded in the history of human civilization, which is characterized specially by transformation of primitive society into modern society. The social transformation has increased both the physical and psychological opportunities for Privacy and also proved to be fruitful for conversion of these opportunities into choices of values in the context of socio-political reality. Social transformation is the responsible factor for changing nature of Privacy as well as the changing character of Privacy violations from primitive societies to modern societies. The comparison of 'Privacy' between primitive and modern societies, establishes that, whatever may be the nature of society, primitive or modern, the need for Privacy or seclusion would always be there, for fulfillment of physical and psychological desires of man.

- **RIGHT TO PRIVACY IN UNITED STATES**

The fast expansion in online communication and commerce over past decades has raised issues and concerns in the United States in an online environment. The term 'Privacy' is not used in the U.S. Constitution or bill of Rights. However, the U.S. Supreme Court has given decisions in favour of the right to privacy from the First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendments to the Constitution of U.S.

A Strand of the right to privacy in United States is the protection against the invasion of the private sphere by government. In the landmark U.S. Supreme Court case of 1965 **Griswold vs. Connecticut** concerned a law made by the State of Connecticut which punished "any person who uses any drug, medicinal article or instrument for the purpose of preventing conception." The appellant was running centre at which information, instructions and medical advice was given to the married persons as to the means of preventing conceptions. Court by extended thinking about privacy to question of bodily autonomy in ruling that information about people's marriages and sexual relations was also protected as privacy right.

As per the research done by the Boston Consulting Group, personal data Privacy is a major issue for 76% of global consumers and 83% of U.S. consumers. 61% of Americans said they want more to protect their right to privacy. The data is being collected by majority of social networking sites people spent time on everyday are not regulated as there are no federal privacy laws regulating many companies, they are quite free to do what they want with the users data, unless a state has its own data privacy law. In most states, companies can use, share, or sell any data they collect about you without informing you or taking consent from you that they are using or collecting your data without your permission. No national law is there to regulate companies that they must notify you if your data is breached or exposed to unauthorized parties. If a company/ social networking websites shares your sensitive information such as your health, location, etc. with third parties (like data brokers), those third parties can further sell it or share it without informing you. The United States does not have a single law regarding the privacy of all types of data rather it has many different laws for different types of data.

- **LAWS RELATING TO PRIVACY IN UNITED STATES OF AMERICA (USA)**
- **Electronic Communication Privacy Act, 1986 (ECPA)**

The USA not only passed ECPA specifically for internet but it is most often used for internet privacy suits. The law prohibits unauthorised international access to facility or networks and the interception of data. If authorisation to access a computer facility exceeds so it falls under an offence. The ECPA provides for criminal and civil penalties for violations. Civil penalties include statutory damages and reasonable coast of the suit that gives rise to many class action suits.

- **Children Online Privacy Protection Act, 1988 (COPPA)**

The COPPA is enacted to protect the privacy of children under the age of 13 while they are net surfing. The act depicts the data that can be collected of a child, first and last name, home or other physical address, e-mail address, telephone number and social security number. The Federal trade Commission (FTC) is authorised to add other categories for information that it determines. The COPPA requires each website operator to obtain verifiable parental consent before collecting, using and disseminating any of the above data. It also provides that the websites not restricts the participation of children in games or no amount should be taken in disclosing that information of children.

- **Video Privacy Protection Act, 1988 (VPPA)**

The Video Privacy Protection Act was enacted to protect the privacy of customer rental and purchase of videos. Although the law did not consider the internet, its language is sufficient to include internet video transactions also. The act applies to any person, engaged in the business of the rental and, sale or delivery of pre-recorded video cassette tape or similar audio visual materials. The statue prohibits the disclosure of purchase or viewing history records of individual customers without their informed written consent in advance of disclosure, with certain expectations. This statue may create the risk for companies streaming video for a fee over the internet. Disclosure of consumer data could leave these companies opens to individual or class action law-suits. The acts provides for statutory and punitive damages.

- **Computer Abuse and Fraud Act, 1986 (CAFA)**

CAFA also known as the anti-hacking statute prohibits unauthorized access to computer system. The statute provides for penalties for unauthorized access and also prohibits exceeding any authorization. Under the CAFA, one may not access the computer with authorization and to use such access to obtain or alter information in the computer that the access of is not entitled so to obtain or alter. Protecting computers includes any computer used in interested communications or commerce. Paragraph (5A) of the statue also prohibits the transmission of virus with the intention of causing damage to protected computer. The violation of this statue carries both criminal and civil penalties. The damages are limited to economic process and the

action must be brought within two years of violation or within two years of discovery of damage. This statue is often relied on in internet privacy class action suites.

- The Health Insurance Portability and Accountability Act, 1996 (HIPAA)

HIPAA is an omnibus privacy act for medical records that mandates the establishment of privacy protection for health care information. HIPAA requires each person or entity who maintains or transmits health information to maintain reasonable and appropriate administrative, technical and physical safeguard to ensure that integrity and confidentiality of the information, protection against any reasonably anticipated threats or hazards to the security or integrity of the information and unauthorized uses or disclosure of the information and ensure compliance by the officers and employees of such person or entity.

- **US Privacy Act, 1974**

US Privacy Act is an old statue when databases were the height of computer technology, Congress and others were concerned about the actual misuse of personal data held by the government and landmark US Privacy Act of 1974 was passed which contained important rights and restrictions on data held by US government agencies. Right of US citizens are to access any data held by government agencies, right to copy that data, right of citizens to correct any of the errors information, etc. But it is restricted to the data that is collected by the US government from its citizens and not on the data that is collected in particular by companies on internet.

- **CASE LAWS**
  - **Roe vs. Wade**

In this case, whether the unmarried pregnant woman has right to terminate pregnancy was considered by Supreme Court of US. The relevant law is of the Texas which prohibits abortions except those which procured or admitted by doctor for the purpose of saving the life of mother. The constitutionality of the law of Texas was challenged that the said law improperly invaded the right and the choice of the pregnant women to terminate her pregnancy and violated her liberty under fourteenth amendment and right to privacy recognised in Griswold. Justice Blackmun who delivered majority opinion upheld the right to privacy as Right to privacy in

not mentioned in the Constitution but the court has recognised the right to personal privacy or guarantees certain area of privacy.

- **U.S. VS. MEREGILDO**

In this case[31], in grand jury investigation, the government applied for a search warrant as the contents of defendant facebook account. Magistrate Judge in the opinion that there is a just and probable cause exists to obtain defendant's Facebook account contents and issued the warrant. The defendant attacked the government's method of collecting evidence to supporting determination of probable cause. The witness was defendant's Facebook friend and gave the government access to the defendant's Facebook profile.

The court states that generally, people have a reasonable expectation of privacy when contents in their home computers but this expectation is not absolute, and may be extinguished when a computer user shares information over the Internet or by e-mail. When a social media user posts any information or anything to the public, they are not protected by the Fourth Amendment. However, postings using more secure privacy settings show that the user wants to preserve information as private and may be constitutionally protected. The defendant posted messages regarding prior acts of violence, threatened violence to rival gang members. Accessing to the defendant's profile formed the core of the government's evidence of probable cause supporting that search warrant.

- **DATA PROTECTION IN UK**
  - **The Data Protection Act, 1988 (DPA)**

The Data Protection Act, 1988 (DPA) is a United Kingdom Act of Parliament. It is the main piece of legislation that governs protection of personal data in UK. Compliance with the act is overseen by an independent government authority, the office of the Information Commissioner. The act defines the eight principles of the information handling practice. The key principles of the act are:

- Data may only be used for the specific purposes for which it was collected.

- Data must not be disclosed to other parties without the consent of the individual whom it is about, unless there is legislation or other overriding legitimate reason to share the information. It is an offence for other parties to obtain this personal data without authorisation.
- Individuals have a right of access to the information held about them, subject to certain exceptions.
- Personal information may be kept for no longer than is necessary.
- Personal information may not be transmitted outside the country unless the individual whom it is about has consented or adequate protection is in place.
- Subject to some exceptions, for organisations that only do very simple processing, and for domestic use, all entities that process personal information must register with Information Commissioner.
- Entities holding personal information are required to have adequate security measures in place. Those include technical measures and organisational measures.

- **The Data Protection Act, 2018 (DPA)**

The Data Protection Act 2018 act of parliament updates the data protection law of United Kingdom. This law complements the European Union's General Data Protection Regulation (GDPR) and replaces the earlier Data Protection Act of 1988. The act has provisions about the processing of personal data, the processing of personal data by the intelligence services, the Information Commissioner, the enforcement of the data protection legislation, Etc. The act also includes new offences that whosoever knowingly or recklessly discloses the information of the personal data without the consent of whose data is being shared and selling and offering to sell of personal data is also falls under category of offence.

- **RIGHT TO PRIVACY IN INDIA**

The digitalized economy has resulted in sharing of personal data, both willingly and unwillingly due to which security breaches and data privacy infringement by the corporations who are in control of the data. There is no specific legislation for data protection and data privacy in India which resulted in corporations to enjoy by using user's data without any fear

of legal actions. The term Right to privacy is not used in the Indian Constitution but interpreted from Article 21. Few other statutory legislations regulating inappropriate disclosure of personal information that is the Information Technology Act, 2000 (IT Act) and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (IT Rules). Apart from that, there are penal provisions under the Indian Penal Code, 1860, which can be invoked indirectly in the instances of data theft.

Further the Government of India in July 2017 formed a Committee under the guidance of Justice B. N. Srikrishna for examination of the concerns regarding data protection. In July 2018, the Committee made a draft called Personal Data Protection Bill 2018, after the draft seeks suggestions from the public, industry experts and other stakeholders. On 11 December 2019 revised draft in the form of Personal Data Protection Bill, 2019 introduced and passed by Rajya Sabha.

- **LAWS RELATING TO PRIVACY IN INDIA**
  - **CONSTITUTION OF INDIA**

In last few decades, there is growth in belief that Constitution contains rights other than expressly mentioned in the constitution. To make presence of such right it is important to show that right in question is integral part of the non-existing right upon which its existence depends. The non existing rights could be called unenumerated rights. If the unenumerated right is a definite and integral part of the enumerated right, then it has as much force as the enumerated right itself. For example, freedom of press has nowhere been expressly provided in the Constitution, it continue to have a very definite presence by the virtue of the fact that it constitutes an indispensible part of Article 19 (1) (a) which guarantees right to freedom of speech and expression in India.

Article 19 (1) (a) and 19 (2) of Indian Constitution reads as follow:

- All citizens shall have the right -
- To freedom of speech and expression
- Nothing in sub-clause (a) of clause (1) shall affect the operation of any existing law, or prevent the State from making any law, in so far as such law imposes reasonable restrictions

on the exercise of the right conferred by the said sub-clause in the interests of [the sovereignty and integrity of India] the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence.

Right to Privacy is not a fundamental right but gained constitutional recognition in India. The Court interprets 'right to life' and 'right to freedom' to establish the right to privacy. Courts have read the right to privacy into the fundamental right to freedom of speech and expression under Art. 19 (1)(a) of the Constitution of India. The Supreme Court of India held that the right to freedom of speech or expression under Art. 19 (1)(a) means the right to express one's convictions and opinions freely by word of mouth, printing, writing, picture or any other manner. It held that if any person is speaking on telephone, he is exercising his right to freedom of speech and expression and any tapping will be violation of his freedom. So, recognising person's right to privacy.

In Kharak Singh Vs. State of U.Pwhile assessing the constitutional validity of M.P Police Regulation providing for picketing and domiciliary visits by the police to the residence of the accused, the apex court held that the right to privacy is not absolute and cannot be a fundamental right guaranteed under the Constitution of India it can be infringed by state for outstanding public interest.

In historic judgement of Puttaswamy v. Union of India, it was held that the right to privacy isa fundamental right and falls within the Article 14, 19 and 21 of the Constitution of India. It particularly exists naturally in the right of life and liberty. It was declared that this is a fundamental and inalienable right that protects all personal information of every individual. Therefore, any act by anyone including the state which infringes the right to privacy of an individual subjects to strict punishment. Also, it was clarified by the Apex court that even the right to privacy is now a fundamental right but it is still subject to reasonable restrictions.
Article 21 of the Indian Constitution lays down the foundation for various rights for the citizens of India and holds significance in a free and democratic society. It is one of the most naturally

growing provisions, the heart of the Indian Constitution which lays down the basis for other laws in India. Right to privacy places itself in Article 21 of the Constitution of India.

- **THE INFORMATION TECHNOLOGY ACT, 2000**

The IT Act, 2000, manages the transactions carried through electronic data interchange and electronic communication. If any negligence in employing reasonable security practices and procedures for using or processing of sensitive personal information so the body corporate held liable. The Act has expressly tried to protect Right to Privacy in the electronic medium and has declared the violation of privacy as an offence under the Act. It has prescribed punishment for violation of privacy under the Act, wherein the amount of fine can be extended upto two lakh rupees. It has clearly specified the concept of Privacy as well as the circumstances amounting to violation of Privacy. Intention of the Act is very clear in this respect that, it has tried to cover both physical as well as electronic privacy, because taking of photographs by means of unauthorized intrusion into the private area amounts to violation of Physical Privacy. But, when those photographs are transmitted through electronic medium, then it amounts to violation of Electronic Privacy. Again, committing unauthorized interference with the electronic records would amount to violation of Electronic Privacy.

IT Act provides for the penalty for unauthorized handling and use of data as:

Any person found guilty of tampering, destroying or stealing any data acquired by unauthorized access; or causes damage to any computer or computer resource with dishonest or fraudulent intention will be held liable for imprisonment up to three years or with fine extending to five lakh rupees or both.

Any person having secured access to e-record, register, correspondence, document or any material, discloses the same will be punished with imprisonment up to two years or with a maximum fine of one lakh rupees or both.

Any person including an intermediary if found guilty of disclosing personal information breaching lawful contract entered with the data provider with intent to cause wrongful gain or

wrongful loss will be held liable with a maximum imprisonment of three years or a maximum fine of five lakhs rupees or both.

The IT Rules 2011 maintains security procedures and provide general guidelines on privacy. Information of a natural person is included in the definition of personal information. Sensitive personal data or information means information relating to passwords, biometric data, medical record, sexual orientation, financial or bank particulars, physical, psychological and mental health status of an individual. These rules widely regulate number of facets of sensitive personal data like consent, collection, use, storage, security procedures for protection, disclosure, transfer, review, update and withdrawal of consent. Further, the IT Rules states theobligations on body corporate which are:

Privacy policy that should be published by the body corporate or by any person in possession of data on their website clearing and fully stating nature and purpose of the information collected, use, disclosure and the security practices adopted to safeguard the information. **Collection** means sensitive information can be collected by any entity only after obtaining the consent of the data provider. The data provider must be aware of the purpose of collection and should be for lawful purpose only. The data provider must be informing about the parties with whom data will be shared along with the details of the data retaining agency. Data can only be retained for the agreed time period. A Grievance Officer has to be appointed by the body corporate. Consent from the data provider or in accordance to contract entered between the body corporate and data provider or for the discharge of a legal obligation by the body corporateis needed before the **disclosure** of the sensitive personal data to a third party . But data can be shared by the body corporate to a government agency for investigation, identification, or prosecution, even without the consent of the data provider. If the third party will ensure a similar level of protection as provided under the IT Rules so any information is allowed to be **transferred** by the body corporate to a third party in India or abroad. After obtaining the consent of the data provider or for the performance of a lawful contract between body corporate and data provider a transfer is allowed.

- **CASE LAWS**

  - **Govind vs. State of Madhya Pradesh**

This was the case where Supreme Court took a pioneering view and recognised the right to privacy as a fundamental right for the first time.

- **Maneka Gandhi Vs. Union of India**

The Supreme Court in this case, once against accepted that the right to privacy as a fundamental right while analysing the scope of the right to privacy, the apex court held that fora right to be fundamental it has to be an integral part of the named fundamental right. Thus, every travel abroad does not become a part of right to freedom of speech and expression every activity necessary for exercise of the fundamental right cannot thus become elevated to the status of a fundamental right.[59] For this reason, concomitant and peripheral rights which facilitate the exercise of the named fundamental right or give it meaning or substance cannot also become a guaranteed right within the named fundamental right. Appling the logic of the court the right to privacy does not form part of the fundamental right to life and personal liberty as a general rule. It would depend on case to case whether the right to privacy could be read into Article 21.

- **CONCLUSION**

In the US, apart from the protection provided by the federal statute, state statute protects an individual's information privacy. A number of states have consumer protection and fraud laws which apply in many cases to breach of privacy and wrong practice data collection. Any company that collect data by the way of internet may face liability in any jurisdiction wherein the internet is available under any or all of these rules.

In comparison to U.S.A., Privacy Laws are not much enriched in U.K. In fact, there has been no existence of Privacy Laws in U.K. before the passing of the Human Rights Act, 1998 and Data Protection Act, 1998. It means, only in the present era, Privacy Laws have been enacted in U.K. to provide remedy for violation of Right to Privacy. Whereas, in U.S.A. Privacy Act has been enacted in 1974, which is long before the passing of the Acts in U.K. Moreover, U.K. has no direct legislation on Privacy like U.S.A. Only legal provisions available in U. K. for protection of Right to Privacy are all indirect legal provisions, even in the present social scenario.