HISTORICAL ANALYSIS OF RIGHT TO PRIVACY

Written by ***Swati Nair*, Crystal Ann George** & Nileena Banerjee******

** 1st year BA LLB Student, National University of Advanced Legal Studies, Kochi, India*

*** 1st year BA LLB Student, National University of Advanced Legal Studies, Kochi, India*

**** 1st year BA LLB Student, National University of Advanced Legal Studies, Kochi, India*

"Privacy is a common value in that all individuals value some degree of privacy and have some common perceptions about privacy. Privacy is also a public value in that it has value not just to the individual as an individual or to all individuals in common but also to the democratic political system…."[1]

ABSTRACT

This paper aims to trace the journey of right to privacy; from being a no-go area to one of the most controversial topics today. The origin of privacy is deeply embedded in the history of human civilization, characterized specially by the transformation of primitive society to modern society. The concept and definition of privacy has changed over the years owing to different factors. In the Indian context, privacy was never an alien entity; it was an integral part of the deep rooted customs of the rich cultural heritage. While, ,the right to privacy in the U.S.A. in the modern period has been primarily based on the Warren-Brandeis article and the search and seizure cases under Fourth Amendment of the U.S. Constitution which finally led to the Privacy Act, 1974. Right to Privacy is a part of Right to Life and Personal Liberty and its violation a matter of concern at the global level. One of the major challenges is that the right to privacy has not been adequately dealt with by the legislation in India or the United States. The current legislations that deal with the protection of the Right to Privacy do not in fact adequately safeguard this right. Assessing the global nature of this issue, it therefore becomes imperative that we deal with this issue transcending geographical boundaries and implement international treaties. Also, considering the fact that we live in an era of information, and not

all of the information we have is required to be shared, certain restrictions, protections and safeguards are required to protect such information. As a result, privacy becomes increasingly important in this technologically advanced era of the twenty-first century. The paper attempts to do a comparative study between the privacy laws in the USA and India and critically analyze the grey areas that need to be worked upon. One of the watershed moments in the context of privacy in India was the 2017 Puttaswamy judgment, which declared the right to privacy as a fundamental right. India still lacks a data protection law that would give meaning to the judgment beyond just being on paper. In the era of technology and data driven governance, privacy has been reimagined and relooked at; it is no longer mere physical intrusion into one's private space rather the invisible threats we face. The concept of privacy has undergone a change world over in the 21st century; it is beyond a man giving a mere isolated life but denotes freedom from unauthorized interference into a person's private sphere.

PRIVACY IN ANCIENT TIMES

The concept of privacy, contrary to common beliefs, is not a modern day notion. It has come a long way from not being mentioned to being one of the most controversial, unsettled and delusional right in the Indian context. In the post-colonial era, arguments on privacy are often based on the premise of perceived alienness of the concept, brought by the colonizers. The fallacy in such an argument is that it ignores the cultural plurality of the concept. Even before the advent of the British, established Islamic and Hindu legal systems, though did not explicitly use the term 'privacy, practiced the ideals of privacy. This concept can be traced back to the "Hitopadesha" and "Dharmashastras" wherein they specify certain aspects like family, worship and sex that had to be protected from public disclosure. Privacy matters when we look at individuals as being part of a larger society. On one hand, society and the individual are interlinked yet on the other hand we need to have mechanisms in place that demarcate the line between public and private. The distinction between ghar and bahar (home and outside) or the famous proverb "sarvas swe swe grihe raja" (every man is a king in his own house) are examples of how relevant privacy was even in ancient times.

The term 'Privacy' is derived from the Latin word 'privatus' which means separated from the rest. Although it is a concept with multiple interpretations and meaning depending on the social context, it technically means the right to be left alone. Due to the changing context, coming up with a specific definition has not been possible, the first attempt to formally define privacy was made in 1890, by Warren and Brandeis in an article titled: "Right to Privacy"[2], in which they defined privacy as the right to be left alone. What is often confused is the nature and context in which privacy is considered now and in the ancient times. Though the term "privacy" per se has not been recorded in the ancient texts nor has the term been used in the context we use it today, it has definitely been in practice in the form of various practices and traditions. The linguistic lacunae is a hurdle in articulating pre-modern notions of privacy but cannot be an argument against the very existence of privacy. For instance, in the Manusmriti there were provisions that prohibited bathing in tanks that belonged to other men and using wells, gardens and houses without the owner's permission. These prohibitions at that time were not driven alone by the notion of privacy. The rationale was that by using others' property one appropriates a portion of their sins. Privacy in this context was interlinked with the concept of purity, though not explicitly mentioned it did secure the right to privacy of the citizens. A person's right to property and privacy in that context is akin to what we see in the modern day legal system. In the Hindu jurisprudence, evidence of this is found in Yajnawalkya Samhita and the Manusmriti that condemn the usage of another person's property without their permission. Further, privacy with regard to bodily integrity was also recognized and this is recorded in the Yajnawalkya Samhita which states, "If many persons know a woman against her will, each of them should be made to pay a fine of twenty four panas". Additionally, the Arthashastra expressly noted that even a commercial sex worker cannot be forced to engage in sexual intercourse. In ancient times, to much of our surprise, women could make a claim of privacy against her husband too and ironically, while the modern society does not treat marital rape as a crime, the *Manusmriti* considered it an offence. And, husbands were not allowed to look at their wives when they were relaxing and needed some time for themselves.

Even the Bible has quotations where privacy was noted even in ancient western societies; where shame and anger led to the intrusion of a person's privacy. The accounts of Adam and Eve, when they started to cover their bodies with leaves, is evidence enough to show the prevalence of privacy during that era. Through a legal prism, the Code of Hammurabi contained a section on intrusion into another person's home. The very idea of privacy traditionally

originated from the distinction between what is "private" and "public". Yet, the boundaries of public and private are ever changing and this has resulted in diverse interpretations on what constitutes privacy. In ancient societies people had low opportunities of self-determination as they were excessively influenced by the State. This is illustrated by Plato in his book, "Laws", where a person's life was determined by the state and there was no scope for individual freedom and autonomy. During the Medieval Age there was no real privacy as an individual existed only as a member of a community and his private life was constantly being "monitored" by the conduct of others. The emergence of "real" privacy is only as late as the 19th century and the subsequent appearance of cities. The changes in the society led to changes in the way people lived and the extent of autonomy they got. This also led to the physical and mental privacy being separated and started to evolve in two different ways.

With the advent of nation states being formed, as a consequence of the post-colonial era, citizens become more aware of their rights and entitlements. Subsequently, States began to organize themselves into a structural and institutional framework and played a more active role in regulating the lives of the people and this often led to abuse of power. It was in this context that the concept of privacy, as we know of it today, came into the picture. Yet, the broad meaning we give to privacy has not been the same since its inception. One aspect that needs a mention is the distinction between 'Privacy' and 'Right to Privacy'. Privacy is a state of affairs or a way of life where individuals are in control of their private life, without interference from others. On the other hand, the right to privacy is to choose and enjoy this state of 'privacy'. Privacy exists in every society as a result of law of nature while right to privacy is a social construct developed based on legal policies and social conventions. The State in the disguise of "in the interest of public" deviated from the principle of privacy in gaining more control over the private life of its citizens. Therefore, it is essential that countries put down mechanisms that act as a check against unjustifiable abuse of power and secure its citizens right to privacy.

EVOLUTION OF RIGHT TO PRIVACY IN INDIA

The Supreme has on various occasions dwelled about the various aspects of privacy before declaring it a fundamental right. As a result of this, the ambit under right to privacy has constantly been widened to include even right to sexual orientation as laid down in the Navtej

Singh Johar v. UOI[3] case and Right to be forgotten, in the Jorawer Singh Mundy v. UOI[4]. However it was only as late as 24th August 2017 that the Supreme Court in Justice K.S Puttaswamy (Retd) v. UOI[5] case held that the right to privacy was a fundamental right flowing from Article 21 under Part III of the Constitution of India. However, like other fundamental rights, the Supreme Court also held that right to privacy can be restricted in well-defined circumstance; (a) if there is a legitimate state interest in putting the restriction (b) if the restriction is proportionate and necessary to achieve that interest (c) if the restriction imposed is in accordance with procedure established by law. The court relied on the precedent given in the Maneka Gandhi v. UOI[6] for reiterating the significance of the three point principle mentioned above and any State action that infringes the right to privacy will be measured against this three-fold test. The judgment was not decided in isolation rather had several implications on matters incidental to the principal issue decided by the Court. It had a bearing on the Navtoj Singh Johar case that decriminalized homosexuality in India, by implying that the right to privacy also included an individual's choice about his sexuality. Secondly, it also went to the extent that the State cannot impose a ban on certain food choices of an individual due to social and religious reasons. Lastly, the judgment also opined upon the various aspects of the multifaceted relationship between privacy and big data companies in the context of how efficient use can lead to State achieving its legitimate interest.

The doctrinal foundation of the right to privacy in India rests on the trilogy of decisions in M.P Sharma v. Satish Chandra[7] (1954), Kharak Singh v. State of UP[8] (1962) and Govind v Madhya Pradesh and Anr[9] (1975). The M.P Sharma v. Satish Chandra case was regarding search and seizure of some documents of a company. There was a writ petition before the Supreme Court that challenged the constitutional validity of the searches on the grounds that they violated Articles 19(1)(f) and 20(3). The 8-judge bench of the Supreme Court held that the Constitution did not subject the power of search and seizure to the fundamental right of privacy. They further observed that, unlike the Fourth Amendment of the Constitution of the USA[10] there was no justification to apply the concept of privacy in search-and-seizures. The case of Kharak Singh v. State of UP dealt with Kharak Singh who was arrested for dacoity and challenged the surveillance by the police. Due to lack of evidence he was later released but the Uttar Pradesh Police brought him under surveillance in accordance with Chapter XX of the Uttar Pradesh Police Regulations. Kharak Singh then challenged the constitutional validity as it violated

Articles 19(1)(d) and Article 21. The 6-judge bench held that domiciliary visits at night was unconstitutional, but upheld the rest of the regulation. Additionally they also held that the right of privacy is not a guaranteed right under the Constitution. In the case of Govind v. State of Madhya Pradesh and Anr, the petitioner alleged false accusations against him on the basis of which he was put under surveillance by the police. The Supreme Court dismissed the petition but advised reform in the Madhya Pradesh Police regulations and observed that they were 'verging perilously near unconstitutionality'.

The decision made in the Puttaswamy case highlights the need for the Constitution to evolve in order to meet the aspirations and challenges of the present age. In an era that is driven by information technology, the Courts must give a liberal interpretation to the concept of individual liberty, especially when an overarching presence of State and non-State entities has a bearing on an individual. Apart from the court deciding on the matter and the legislations that were enacted subsequently India is also signatory to various International Conventions that deal with the right to privacy: The Universal Declaration of Human Rights(1948)[11], The International Covenant on Civil and Political Rights(1966)[12] and The European Convention on Human Rights(1953)[13]. One of the key bills that needs a mention in the context of privacy is the Data protection Bill (2019)[14]. The primary objective of the Bill was to provide protection of personal data of individuals, and establish a Data Protection Authority for the same. The Bill governs the processing of personal data by the following entities: (i) government, (ii) companies incorporated in India, and (iii) foreign companies dealing with personal data of individuals in India. The Bill also clearly defines what constitutes personal data to prevent any ambiguity and varied interpretations; personal data is data which pertains to characteristics, traits or attributes of identity, which can be used to identify an individual. Further, the Bill allows processing of data by the above-mentioned entities subject to the consent of the individual (however, exception is given in certain circumstances where data can be collected without consent like (a) required by the State for providing benefits to the individual (b) legal proceedings (c) to respond to a medical emergency).

It is high time we pass legislation that provides for security mechanisms to prevent the misuse of data without legitimate state interest. India, is one of the few countries in the world that still does not have a robust law concerning data privacy even after the Court has declared it as a fundamental right back in 2017. Being a democracy in the 21st century where technology is as

much in control of us as we are, it becomes paramount that the State does not get a leeway in misusing data in the disguise of larger "public interest". The Bill in its current stage definitely has its flipsides but the cost of not having a legislation is much more than implementing a legislation and working on the loopholes as we move ahead to make it more effective.

ORIGIN OF THE RIGHT TO PRIVACY IN US

Neither the US Constitution nor the Bill of Rights explicitly contained any provisions relating to the right to privacy. The Supreme Court has said that some Amendments open out to the right to privacy. The Constitution, through the Fourth Amendment, protects people from unreasonable searches and seizures by the government. The Fourth Amendment, however, is not a guarantee against all searches and seizures, but only those that are considered as unreasonable under the law. In 1890 the Harvard Law Review published the essay of Samuel Warren and Louis Brandeis. Their essay stemmed from their concerns about an individual's privacy which was threatened by various inventions, particularly photography. They found photography to lead to "the unauthorized circulation of the portraits of private people" and that right to privacy is a "right to be let alone"[15]. It stood for the establishment of the right to privacy and is considered as one of the foundation stones of this right.

The UN Declaration of Human Rights 1948 has Article 12 which explains that no man's privacy shall be arbitrarily interfered and every man shall be protected by law against such interference[16]. The *Griswold v. Connecticut* case[17] was one of the first to discuss the right to privacy in the US. In this case the concept of marital privacy was analyzed and the court held it as a Constitutional right but struggled to recognize the source of the right. The Court held that the right can be derived from the First, Third, Fourth and Fifth Amendments. The Court found the Connecticut law which banned people from using drugs to prevent conception as unconstitutional and a violation to right to privacy. This was further discussed in the *Roe v. Wade* case[18] in 1973 when the Court said that a woman has a right to terminate her pregnancy and not providing such a right would violate the right to privacy mentioned in the *Griswold v. Connecticut* case. Later the *Katz v United States*[19] case framed the Katz test, a two part test to determine the reasonable expectation of privacy. First, is when a person actually exhibits an expectation of privacy and the second, is that the society is ready to recognize this expectation

as reasonable; that is, a man can expect a reasonable right to privacy in his home but things he exhibits in plain view does not come within the scope of right to privacy. This was adopted as a formulation for the Fourth Amendment search analysis in *Smith v. Maryland*[20].

The Court then further extended the right to privacy provided in Griswold v. Connecticut case in the *Eisenstadt v. Baird*[21] to the use of contraceptives by unmarried individuals. The Court held that the right to privacy should not be limited to married couples, but to all to be free from "unwarranted government intrusion". In 1974, the Family Education Rights and Privacy Act (FERPA) was brought to deal with the privacy of the student education records. Educational institutions must have the consent of the parent or the student (in some cases) to release the information in the records. The Act extends to even the parents being disallowed to view the records of their ward without the student's consent if (s)he is above 18[22]. During the same time the Privacy Act[23] of 1974 was brought. This Act regulates the actions of the federal agencies that use personally identifiable information. This Act prohibits the agencies from publishing or disclosing the information of an individual without the written consent of that particular individual. The Section 5 of the Privacy Act 1974 led to the establishment of US Privacy Protection Study Commission for the purpose of making recommendations to improve the Act[24]. The Commission issued the Privacy Commission Report and concluded its works in 1977.

In 1986 the Telephone Consumer Protection Act[25] and the Do-Not-Call Registry was made. The former imposes restrictions on calls made for the purpose of inducing a consumer to buy a particular product (telephone solicitations) and the latter provided an option for consumers to opt out of such calls. The government maintains a registry of the numbers of the people who have requested to not be contacted as part of telemarketing. The Act focuses on respecting the privacy of the consumers who wish not to be disturbed by such calls or robocalls. Health Insurance Portability and Accountability Act of 1996[26] contained provisions regarding the protection of personally identifiable information maintained by health care institutions and insurance providers. It prohibits disclosing information regarding the patient to anyone except the patient itself or the authorized representative of the patient. In 1998 the US Federal Government enacted the Children's Online Privacy Protection Act[27]. It explains the practice of collecting the personal information of children under 13 years by websites and what all must be the components of the privacy policy and the responsibilities of the operator with respect to

the child's privacy. The Act disallows the websites that collect personal information, particularly social media sites, to be used by children under 13 even if they have their parent's consent. The Act has been widely criticized for being not effective and encouraging age fraud by prohibiting children under 13 years of age to use some websites. The Clinton government created a new post called Chief Counselor for Privacy for managing the information privacy laws in 1999.

The Gramm-Leach-Bliley Act or the Financial Services Modernization Act was also brought in 1999. As per the Act, there must be complete compliance to the provisions of this Act irrespective of whether it was disclosure of non-public information or not and that there must be a policy in place to protect the data from threats to security and data integrity[28]. It also mandates that every financial institution share a privacy notice with their consumer regarding where and how the information about the consumer is used and how it will be protected. In *Kyllo v US*[29]. The court found that using thermal imaging devices at a private house constitutes a house search and is a violation to the right to privacy even if it is used to determine any non-intimate activities since it can also catch intimate activities. The E-Government Act made in 2002 had provisions relating to protection of personal privacy and national security. It mandated all federal agencies to conduct a Privacy Impact Assessment that collects and stores personally identifiable information[30]. In 2010, the Red Flag Identity Theft Protection Rule was created by the Federal Trade Commission. It mandates financial organizations to have a policy to prevent identity theft by identifying "red flags".

The *United States v. Jones*[31] held that the GPS surveillance of a car would constitute as an invalid search that violates the privacy of that individual. The court also said that the people's expectations of privacy are changing with the advent of technology. The court further unanimously held in the *Riley v. California*[32] case that searching the digital contents of a cell phone without a warrant is unconstitutional. The court found that the modern cell phone is an instrument of convenience and held the "privacies of life" for many Americans. In the 2020's various states like California and Virginia have enacted legislations relating to data protection and privacy of individuals. It is evident that the concept of privacy and intrusion has shifted over the years and this has been reflected by various case laws and legislations.

COMPARATIVE ANALYSIS OF RIGHT TO PRIVACY IN INDIA AND US

The excess of privacy and surveillance laws in the United States, especially in the aftermath of 9/11, and the lack of the same in India provides for an outstanding analysis. The right to privacy in the United States has similarities to that of India by reason of absence of an express right to privacy in the Bill of Rights of the United States of America, and in Part III of the Indian Constitution. The Supreme Court of India, through various decisions, like in the cases of Kharak Singh vs State of Uttar Pradesh[33] and Govind vs State of Madhya Pradesh[34], has recognized that right to privacy to be derived from constitutional rights to expression, personal liberty and free movement within the nation. This right, however, is not an absolute right, and it did not address information privacy. Similarly, the United States Constitution also does not contain an explicit right to privacy, but the Bill of Rights does reflect certain aspects of privacy, like privacy of the person and possessions as against unreasonable searches (4th Amendment), privilege against self-incrimination, which provides protection for the privacy of personal information (5th Amendment)[35] and privacy of beliefs (1st Amendment)[36]. The authority of search and seizure in India is unaffected by the basic right to privacy, according to the Indian Constitution. The Supreme Court of India on this matter, went on to say that, unlike the US Constitution's Fourth Amendment, there was no rationale for using the idea of privacy in search-and-seizure cases.

Following the major 9/11 terrorist attack, United States was forced to enact legislations on matters of privacy and surveillance. As a result, national security was used as the overarching justification, with which many important constitutional concerns like privacy and individual liberty were moved to the side, and draconian laws like the PATRIOT Act[37] and the subsequent use of surveillance and interception were validated. The use of the PARTIOT Act is not limited to counter terrorism, but it has been extended to have broader authority in ordinary criminal and investigative issues. Similarly, even in the Indian scenario, the government considers many amendments to the pending Privacy Bill and strives to gauge public opinion in order to legitimize it, but the looming prospect of a national security threat remains a constant theme in any such campaign. In both of these countries, the priority accorded to 'national security' over individual liberty appears to be an accepted norm. In India there is a lack of a general legislation governing data protection, but on the other hand, the United States has many. The Information

Technology Act (IT Act 2000)[38] was approved by the Indian government in May 2000, and it is a package of regulations aimed at creating a complete regulatory framework for electronic commerce. This Act, however, does not have any specific provisions for the protection of personal data. The United States, on the other hand, has several sector-specific regulations to safeguard children's internet privacy, student education data, private financial information, and people's medical records.

Self-regulatory activities in both countries are helping in creating a better privacy environment. The National Association of Software and Service Companies (NASSCOM) in India is building a database known as "Fortress India" in response to incidents in which workers of BPO companies exploited customers' personal information. This database will allow firms to check out potential workers with criminal histories in an attempt to prevent incidents of employees exploiting customers' personal information. NASSCOM is also a member of the review group for amending the Information Technology Act of 2000. Similarly, the Federal Trade Commission (FTC) in the United States has been pressuring businesses to develop self-regulatory privacy safeguards and adhere to a set of privacy principles. Industry groups have also created a number of privacy seal initiatives.

In the United States there exists a well-structured system of rules and laws that check threats to data privacy within and outside their territorial jurisdiction but in India, such a regulatory framework is still missing. Even though we have the IT Act 2000, it was not enacted to deal with data privacy, fails to specify a list of governmental agencies and is limited to sensitive personal data. The exponential boom in the number of internet users during the pandemic and the subsequent lockdown has given rise to a huge array of data privacy issues where people have disclosed their personal data without a second thought on the repercussions. It cannot be said that there is a complete lack of privacy protection in India. Both, in the USA and India there is no Constitutional provision that directly deals with privacy and at this juncture the Judiciary in these countries have played a very crucial and proactive role. The Courts have interpreted the Constitutional provisions and the rights enshrined therein giving it a liberal meaning to widen its scope and incorporate the aspect of right to privacy. Moreover, there have been several controversial legislations enacted in these countries like the Freedom of Information Act 1966 and the Information Technology Act 2000 in the USA and India respectively. Though these legislators seek to provide the general public information about the

governmental secrets in order to maintain transparency and accountability it has given rise to controversies as governmental records contain personal information of citizens also. In this scenario a new controversy has been raised regarding balancing the Right to Privacy and the Right to Information against one another. Therefore, at the present juncture it is imperative that both the countries work towards enacting more robust laws that act as curbs against unauthorized infringement of the right to privacy of its citizens.

PRIVACY IN THE MODERN TIMES

In the 21st century, with the advent of technology, the answer to what extent an individual has privacy is open to debate. The concept of invading one's privacy has evolved over the years. Earlier it involved a physical intrusion which is no longer necessary. Data privacy is a concept which bloomed over the last few decades and it involves digital profiling, cyber stalking, etc. Data scraping is a method by which advertisers track the user's online activities and sometimes personal chats to provide them with advertisements that might appeal to their interests. Multiple apps of Facebook have been accused of leaking a consumer's personal information without the user's consent to tracking or advertising companies. It is without a question of doubt that the Internet has made it easier to obtain and share data. Though many assume that the internet provides anonymity, they brush aside the fact that it was designed to share information.

The notion we have regarding our control over our personal data is imaginary. Often commercial entities are provided with this information without our consent. In many countries the existing privacy laws were written even before the dawn of the internet. They thus lack enough robustness to protect an individual's privacy especially because the privacy of an individual has taken multiple dimensions over the years. Even now 24% of the countries do not have any Data Protection Legislation. But in many countries it has been accused that the government itself is violating an individual's right to privacy. For instance, in 2013, Edward Snowden, an employee of the National Security Agency leaked information which led to revelation about the surveillance programs of the NSA and the Five Eyes Intelligence Alliance group (consisting of Australia, Canada, UK, US, New Zealand) along with many telecommunication companies and European governments.[39]

Recently, the Indian government was accused of using the Pegasus spyware for surveillance against 300 individuals. Pegasus was initially used to track criminals and terrorists, but now it has become a tool for the government against human right activists, politicians. Pegasus spyware has also been reported to be used by Israel, France, Hungary, Mexico, Saudi Arabia[40].Over the years the legislations of some countries have managed to evolve with the new challenges that technology has posed to data privacy. For instance, in the General Data Protection Regulation Section 32 explains Security of Processing while, California has enacted the California Privacy Rights Act, while the Information Technology Act 2000 in India is not specifically for data protection is used as regulatory mechanism along with Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. Section 43A, 72 and 72A are some of the Sections which deal with data protection and data privacy in IT Act 2000. As mentioned earlier, the Data Protection Bill 2019 comes with a lot of pros but not without its share of cons. One of the main criticisms the Bill has faced is with respect to data localization, which requires the data to be collected and stored before it is transferred to another country. Another criticism that the Bill faced was that it gave the government blanket powers to access an individual's data. After the Snowden revelations, the US federal government enacted the US Freedom Act which imposed certain restrictions on collecting the telecommunication data of US citizens by government security agencies.

It is evident that these countries have attempted to enact legislations for data privacy and data protection. Though these are much needed legislation, they very rarely hit the bull's eye. It might be because the law fails to address the main issue or it fails in its implementation. But such legislation will not help in preventing future incidents like Pegasus. It is important for individuals to believe that their personal data will be stored and maintained properly for them to use the technology comfortably. Technology is the future of the world and it is not possible to abstain from using it, but at the same time threats to data privacy cannot be ignored. Thus, a comprehensive legal policy framework to address data protection and privacy issues, with effective implementation, is the need of the hour.

ENDNOTES

1. Priscilla M. Regan, Legislating Privacy : Technology, Social Values, and Public Policy, 1995, pp.213, 225.
2. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harvard L.R. 193, (Dec. 15, 1890).
3. Navtej Singh Johar v. UOI, AIR 2018 SC 4321.
4. Jorawer Singh Mundy v. UOI, W.P. (C) 3918/ 2020.
5. Justice K.S Puttaswamy (Retd) v. UOI, UOI, 2019 10 SCC 1.
6. Maneka Gandhi v. UOI, AIR 597, 1978 SCR (2) 621.
7. M.P Sharma & Ors v. Satish Chandra, AIR 300, 1954 SCR 1077.
8. Kharak Singh v. State of UP, AIR 1295, 1964 SCR (1) 332.
9. Govind v. Madhya Pradesh & Anr, AIR 1378, 1975 SCR (3) 946.
10. U.S.Const. amend. IV.
11. Universal Declaration of Human Rights, 10 December 1948.
12. International Covenant on Civil and Political Rights, 16 December 1966.
13. European Convention on Human Rights, 4 November 1950.
14. The Personal Data Protection Bill, 2019.
15. Supra note 2.
16. Supra note. 12.
17. Griswold v. Connecticut , 381 U.S. 479 (1965).
18. Roe v. Wade,410 U.S. 113 (1973).
19. Katz v United States,389 U.S. 347 (1967).
20. Smith v. Maryland, 442 U.S. 735 (1979).
21. *Eisenstadt v. Baird*,405 U.S. 438 (1972).
22. En.wikipedia.org. 2022. *Family Educational Rights and Privacy Act - Wikipedia*, https://en.wikipedia.org/wiki/Family_Educational_Rights_and_Privacy_Act [Accessed 30 May, 2022].
23. Privacy Act, 5 U.S.C.§ 552a, (1974).
24. Id.
25. Telephone Consumer Protection Act, 47 U.S.C. §. 227. (1991).
26. Health Insurance Portability and Accountability Act 100 Stat. 2548, (1996).
27. Children's Online Privacy Protection Act, 15 U.S.C 6501-6505, (1988).
28. Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809, (1999).
29. Kyllo v US,533 US 27, (2001).
30. The E-Government Act, 116 STAT. 2899, (2002).
31. United States v. Jones,565 U.S. 400, (2012).
32. Riley v. California, 573 U.S. 373, (2014).
33. Kharak, AIR 1295, 1964 SCR (1) 332.
34. Govind, AIR 1378, 1975 SCR (3) 946.

35. U.S. Const. amend. V.
36. U.S. Const. amend. I.
37. USA PATRIOT Act, Pub.L.No. 107–56 (2001).
38. Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
39. Wikimedia Foundation (2022), Edward Snowden. Wikipedia. https://en.m.wikipedia.org/wiki/Edward_Snowden#Snowden_response_to_Criminal_Complaint, [Accessed May 31,2022].
40. Wikimedia Foundation. (2022). Pegasus (spyware).Wikipedia. https://en.m.wikipedia.org/wiki/Pegasus_(spyware), [Accessed May 31,2022] .