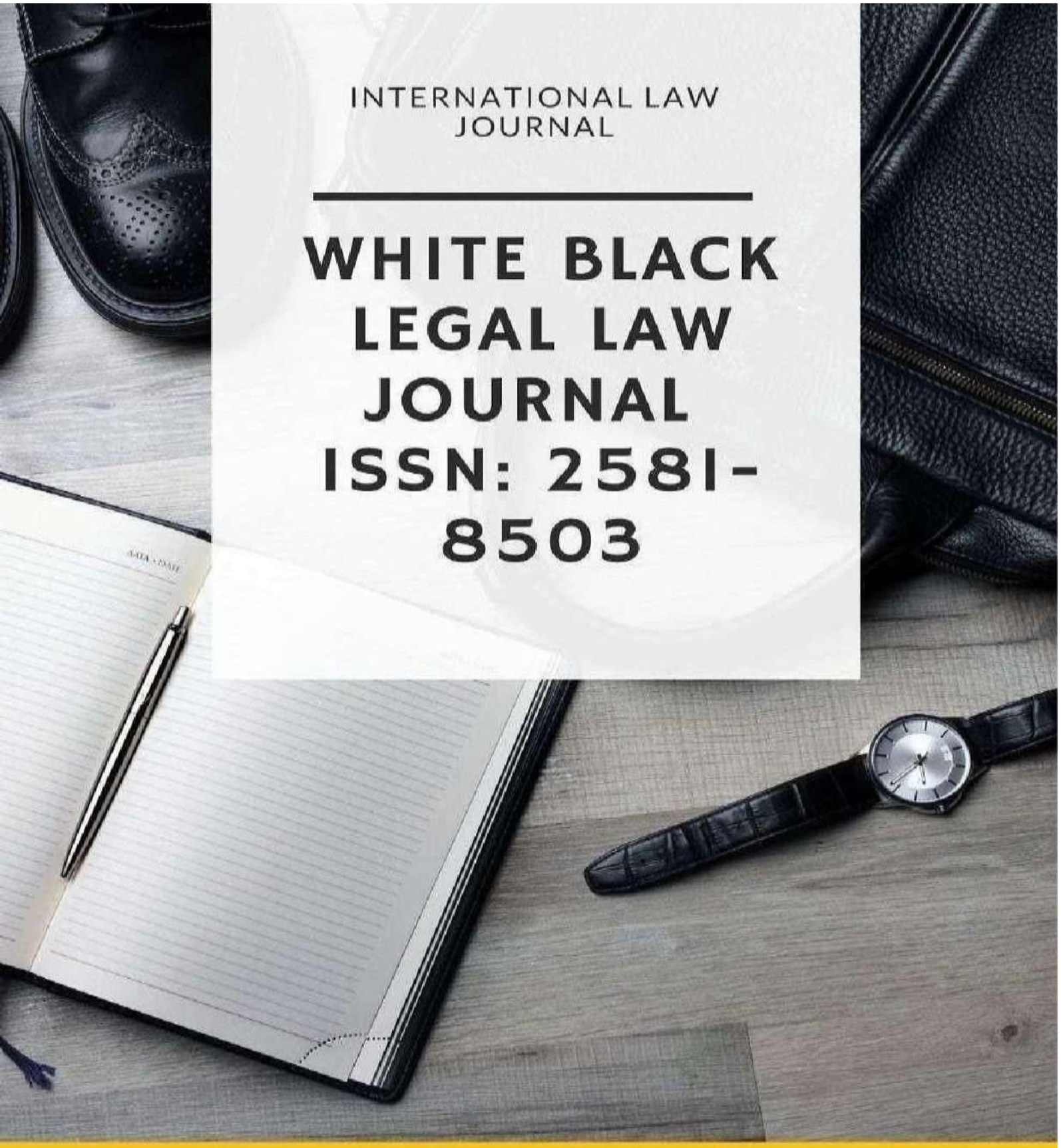

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in ‘Intercountry adoption laws from Uttranchal University, Dehradun’ and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

www.whiteblacklegal.co.in
Volume 3 Issue 1 | May 2025 ISSN: 2581-8503

EVOLUTION OF THE RIGHT TO PRIVACY IN INDIAN CONSTITUTIONAL JURISPRUDENCE- FROM M.P. SHARMA TO PUTTASWAMY TIMELINE

AUTHORED BY - DINESH KUMAR T[1],
PUGAZHENTHI J[2] & PACHAMUTU S J[3]

Abstract:

In the contemporary digital era, the right to privacy has assumed unprecedented significance, intersecting complex domains of constitutional law and rapidly evolving technologies. This research critically examines the scope and nature of the right to privacy in India, focusing on its constitutional foundations and the challenges posed by technological advancements. The right to privacy is recognized as a fundamental right in many jurisdictions, its application in the digital realm presents new challenges due to the sheer volume of data collected and the potential for misuse of this information. Constitutional frameworks, like the Indian Constitution's Article 21, provide a foundation for privacy protection, but these frameworks need to be adapted to the evolving technological landscape. Technological advancements have blurred the lines of privacy, making it crucial to develop robust legal and ethical frameworks to safeguard individual freedoms in the digital age. With the increasing digitization of personal data, concerns related to surveillance, data breaches, and misuse of personal information have intensified. The study analyses key judicial pronouncements, notably the landmark K.S. Puttaswamy v. Union of India judgment, which recognized privacy as a fundamental right under the Indian Constitution. It further explores the implications of technologies such as Aadhaar, artificial intelligence, social media, and data analytics on individual privacy. By comparing national frameworks with global privacy standards and emerging data protection laws, the paper seeks to propose balanced legal and policy approaches to safeguard privacy without impeding innovation. The analysis underscores the urgent need for a comprehensive, enforceable data protection regime that aligns constitutional values with technological realities.

[1] Assistant Professor, Dept of Legal Studies, Vels Institute of Science, Technology and Advanced Studies, Chennai.
[2] Assistant Professor, Dept of Legal Studies, Vels Institute of Science, Technology and Advanced Studies, Chennai.
[3] Assistant Professor, Dept of Legal Studies, Vels Institute of Science, Technology and Advanced Studies, Chennai.

Keywords: Right to Privacy, Constitution of India, Digital Technology, Data Protection, Surveillance, Aadhaar, Fundamental Rights, Cyber Law

INTRODUCTION

One of the cornerstones of fundamental rights in many legal systems across the world, including the Indian Constitution, is the right to privacy. Under Article 19 of the Constitution of India, which addresses the restoration of marital rights and gives people the option to petition the Supreme Court in the event that their fundamental rights are violated, emphasizes the value of privacy. In the current digital era, privacy has taken on even more importance since it includes safeguarding against unauthorized access to one's personal information and affairs. Privacy in the digital realm is crucial for individuals to lead happy and peaceful lives. Each person possesses their own set of secrets and personal information that they prefer not to divulge to others, as it could potentially tarnish their reputation or cause harm. The Supreme Court of India has consistently recognized and upheld the right to privacy, emphasizing its paramount importance in safeguarding individual autonomy and dignity As individuals increasingly interact with digital platforms for communication, commerce, healthcare, governance, and social networking, vast amounts of personal information are collected, stored, analyzed, and shared—often without explicit consent or awareness. This shift from physical to digital interaction has rendered traditional understandings of privacy inadequate and raised concerns about surveillance, data breaches, algorithmic profiling, and the commodification of personal data.

The constitutional recognition of the right to privacy in India came after decades of legal ambiguity, culminating in the landmark judgment of Justice K.S. Puttaswamy v. Union of India (2017), wherein a nine-judge bench of the Supreme Court unanimously held that the right to privacy is a fundamental right under Article 21 of the Indian Constitution. This landmark decision redefined privacy as intrinsic to life and personal liberty, thereby mandating the State and private entities to uphold informational autonomy and dignity in the digital realm. However, despite this constitutional recognition, India continues to face significant challenges in implementing effective legal and technological safeguards to protect privacy. Emerging technologies such as biometric identification (e.g., Aadhaar), artificial intelligence, big data analytics, and automated decision-making systems have deepened the complexities of privacy protection. Additionally, the absence of a comprehensive and

enforceable data protection law further exposes individuals to the risk of misuse and exploitation of personal information by both governmental and non-governmental actors.

Every person has certain thing aspect or anything about there lives that they want to keep it to themselves to not share such thing with the world. It can be anything irrespective of whether it is serious or trivial. it's innate in us to want to take certain facts in certain details about our lives and keep them to ourselves and only release them to people that we trust people that we value and people that understand us but as we move forward in time where the ability to control that information is becoming less and less easy we have to ask ourselves how do we protect those facts how do we keep our privacy in a digital age.

Throughout mankind privacy as a concept has remain the same but privacy as a practice or an action has changed significantly. With the advancement in technology and emergence of internet privacy has certainly changed. The way we communicate, work, study has changed because of the internet. How we perform daily activities has changed. We can gather any information with a click of a button at any time. We can talk with people from all over the world on social media. Internet has made our life certainly easy but there is a price to pay for all this luxury. The price we have to pay for all this luxury is our privacy. What a person wants to share with the world is not entirely upon him. There have been numerous cases throughout out the world where data has been leaked for eg Air India data breach where Hackers gained access to Air India's database in February 2021 and took 4.5 million customers' personal data with them, CAT data breach, Upstox data leak, Police exam data spill (2019) and Cyberabad data theft (2023) As we head into an era in which we are inherently connected, via the Internet of Things, to our devices and each other, privacy will become an even more disparate and complex landscape. We need to move forward into this new age with a better understanding of how to ensure privacy rights are protected and preserved.

WHY RIGHT TO PRIVACY MATTERS

Many individuals believe that they shouldn't have to worry about their privacy on the internet if they have done nothing suspicious. This perspective on right to privacy is incomplete since it doesn't matter if you have done anything wrong or not because your information can still be used against you in way that it might harm you.

Dr. Sidney Gerard, who did a lot of his privacy research back in the 60s and 70s as technology really started to come on board, wanted to study the personal aspect of it. He studied groups of people who had limited privacy rights but not just prisoners. He took people and studied them in environments where they couldn't shield facts where they couldn't present the face they wanted to present and what he found that those people had higher incidences of depression anxiety and then often times it manifested in physical pain. The important aspect of dr. Gerard's research is that invasion of privacy affects each of us individually whether we realize it or not.

WHY RIGHT TO PRIVACY HAS BECOME A BIGGER CONCERN IN THE DIGITAL AGE

It's late at night, you enter and lock the front door behind you. Doors are shut, curtains are closed and doors are locked just before you go to bed. This is what you do to protect your identity, privacy and the artifacts that make up your life. Although our privacy at home is covered by drawn blinds, closed doors and thick walls, the digital walls covering our online lives are now much transparent. Many who sit behind these glass walls, consisting of businesses, algorithms and employees, large thousands of people, hold a constant need for our personal information, data and behaviors as it drives their business models.

Before internet there were not a lot of avenues for people to share their thoughts or ideas. We didn’t have access to information from all over the world. We shared information with less people. Now can we share our data regularly over the web. Privacy before internet was a physical concept. Now with our data spread all across the world privacy has is not merely physical. We’ve created digital footprints which are spread all across the web. Data has become a commodity in the digital age.

HOW ARE WE SHARING PRIVATE INFORMATION IN THE DIGITAL ERA[4]

When joining tournaments, building various profiles and connecting services out of convenience, many of us are eager to place our personal data at the feet of social media ghosts like Facebook. If it's likes, dislikes, partnerships, behavioral features or political leanings,

[4] Lior Jacob Strahilevitz, Social Network Theory of Privacy, The University of Chicagol, Rev (3) 919-988 (2005)

Facebook is a gold mine for advertisers searching for data from users. Whenever we download a new app we never bother to look at the terms and condition. We just tick the box (I have read all the terms and conditions mentioned above). You give access to these app to know your contact information, location, images. Basically, you give access to most of the information present in your phone.

HOW OUR PRIVATE INFORMATION CAN BE USED AGAINST US BY COMPANIES, GOVERNMENT

If a company has personal data (your interests, your political stance, what makes you happy, what makes you sad, etc.) and a means of reaching out to its audience (targeted ads, social media, etc.), then they may have a huge influence not only on individuals but society in general. An argument is made that what's wrong with companies using data for marketing or to sell their product. The problem is the influence they can have on an individual or society with the information they possess. The more information you have about someone, the easier it will be to trick them into believing anything you want them to believe and to lie to you. You only need to show them the part of you that you know they'll like; you no longer need to present a positive impression of yourself generally. The digital world is monopolistic as well. Worldwide, the majority of people utilize one search engine, five social networking platforms that cater to most users, and one single shopping marketplace. Due to their predominance in the market, this has resulted in a scenario where relatively few corporations have control over significant amounts of information. Also, the data that exist in these platforms is not entirely safe as it is prone to hacks. There have been several instances of data breach India over the last few years.[5] Data breaches that occurred in India between 2022 and 2023 demonstrate how susceptible the country is to cyberattacks in a number of industries:

- AIIMS hack. In December 2022, a hack occurred at the All India Institute of Medical Sciences (AIIMS), leading to the encryption of 1.3 gigabytes of data.
- MoChhatua Breach: Sensitive user data was exposed in May 2023 due to a breach that occurred on the Odisha local governance app Mo Chhatua.
- Zivame Data Breach: A security breach at the online women's clothing retailer Zivame exposed 1.5 million customers' personal information.
- Cyberabad Police Data Leak: In April, a significant hack revealed 66.9 crore

[5] Lior Jacob Strahilevitz, Social Network Theory of Privacy,

people's and organizations' data, which resulted in the apprehension of a person suspected of data theft.

- Swachhta Platform Hack: In September 2022, a breach on the Swachh City platform revealed sensitive user data.

Data is used by companies for targeting ads. Targeted advertisements can be utilized to promote unhealthy meals to the fat, dubious medical procedures to the sick, and junk goods to the scientifically ignorant.

CAMBRIDGE ANALYTICA CASE

By using Facebook User's personal information to create psychological profiles, Cambridge Analytica was able to manipulate behavior and deliver precise political messaging. Through an analysis of customers' habits, likes, and other data, the company developed comprehensive profiles to forecast political views. With the use of these profiles, accurate microtargeting was made possible, enabling customized political ads to target particular demographics. By applying psychological insights to its persuasion strategies, Cambridge Analytica was able to increase their efficacy and perhaps impact users' political opinions and behavior. The controversy called into question how data privacy laws should be implemented in the digital era and brought attention to the moral dilemmas associated with using personal information for political purposes.

PRIVACY INVASION BY GOVERNMENT

In the digital era, governments hold enormous authority by gaining access to private information to provide safety and protection. After the Edward Snowden case we have learnt that government agencies have unprecedented access to our personal data. However, the scope of this power raises basic concerns about individual privacy rights and the appropriate bounds of government authority. While governments have a responsibility to protect their populations from a variety of dangers, including terrorism, cybercrime, and public health catastrophes, the techniques used must be guided by legality, proportionality, and accountability. There has to be a balancing of individual interest and societal interest. With fast technological advancements, governments have gained unparalleled access to people's everyday lives and activities, and this will continue. If surveillance is unregulated, particularly without clear monitoring and accountability, governments may gain too much power and potentially abuse

it. This may jeopardize democratic principles and the liberties we cherish.[6]

Historical context of Privacy Rights in India

Article 21 of the Indian Constitution guarantees the protection of life and personal liberty to every individual. It states, "No person shall be deprived of his life or personal liberty except according to a procedure established by law." This provision has been interpreted expansively by the judiciary to include various facets of human life and dignity, and over the years, it has come to encompass the right to privacy as an integral component of personal liberty.[7]

Privacy in India during ancient period

Privacy was practiced in India only when an individual or more people engage in specific private matters. Only this concept of privacy can be traced back to the ancient Hindu texts. As given in texts of Hitopadesh[8], certain matters like worship, sexual intercourse between husband and wife, personal family matters should be protected from getting disclosed and absolute privacy must be given to people engaged in them. Ancient Indian law had a provision which said 'sarve sve sve grihe raja' which means every man is a king in his house. As far as I am able to interpret this means that the man is responsible to protect his family and the events going on inside his house. Thus, responsibility of personal things like worship, sex and family matters not being disclosed, is upon the man of the house.

United states of America

Privacy right was recognized in early days of colonial America. Though not in express terms, but an American court had taken note of this right while deciding De May v. Robertsin 1881. The issue therein was that a physician allowed a "young unmarried man" not schooled in medicine to be present while the plaintiff gave birth. The court reasoned thus, "It would be shocking to our sense of right, justice and propriety to doubt even but that for such an act the law would afford an ample remedy. To the plaintiff the occasion was a most sacred one and no one had a right to intrude unless invited or because of some real and pressing necessity". The words "no one had a right to intrude" might technically be varied from "right to privacy" as such in as much as the lady giving birth in this case should be entitled that right; but the

[6] The Right to Privacy in Nineteenth Century America, 94 HARV. L. REV. 1892, 1894 n.18 (1981).
[7] https://www.youthkiawaaz.com/2021/10/save-yourself-from-intrusion-know-your-right-to-privacy
[8] https://www.thestatesman.com/features/the-privacy-paradigm-1501117433.html

disallowance of non intrusion appears to be a duty in substance and hence a corollary right of privacy might rest with the woman. The maxim that everyone's home is his castle is been in place from as early as 1499.That view was asserted in Semayne's case.

In United States, congress is believed to have passed a law prohibiting non recipients from opening a mail. The evolution of law with regard to privacy that was similar to that of common law took a major turn with the amendments of Bill of Rights in the United States Constitution. The third, fourth and fifth amendments to the U.S. Constitution have nexus with privacy rights, though not expressly.[9]

The Third Amendment protects the privacy of the home by preventing the government from requiring soldiers to reside in people's houses (employing Blackstone's castle theory); The Fourth Amendment provides broad limitations on the government's power to search and to seize; The Fifth Amendment affords individuals a privilege against being compelled to testify about incriminating information. It is submitted however, that the amendments are concerned with right against encroachment on private space and none of these employ privacy with regard to dissemination of information. Further, the amendments being a part of U.S. Constitution imposes the duty on the state and does not govern the private interaction in so far as right to privacy is concerned. It was in 1890 that Warren & Brandies's article "The Right to Privacy" was published in Harvard Law Review that had the effect of "adding a chapter to law"

United Kingdom

At common law, the concept of privacy existed since 15th century as Blackstone suggests that the house of the man was to be his castle. Blackstone defines privacy as "listen under walls or windows, or the eaves of a house, to hearken after discourse, and thereupon to frame slanderous and mischievous tales". Nevertheless, despite right to privacy being recognised by scholars at common law, it is ironic how there was no remedy for the breach of such right under Tort Law. According to Winfield Jolowicz on Torts, There is no direct action for privacy under English Tort Law. However, though there is no direct protection under English Tort Law from breach of privacy, relief is usually granted under some other tort. This can be illustrated by taking the example of Argyll v. Argyll[10] wherein the duke was not allowed to

[9] The Right to Privacy in Nineteenth Century America, 94 HARV. L. REV. 1892, 1894 n.18 (1981).
[10] Prince Albert v. Strange, 64 Eng. Rep. 293 1815-1865.

publish secrets of his marriage to the Duchess of Argyll. Hence, though English law might not mention "privacy" in express terms, but it has a framework that protects injuries caused as a result of breach of privacy, in substance.[11]

There are other specific statutes also that embody the concept of privacy including Interception of Communications Act, 1985 that regulates phone tapping and Data Protection Act, 1998 that regulates privacy of data collected for a specific purpose. Most relevant out of these for the present context is the Data Protection Act, 1998.

India

The right to privacy was in a benign stage and existed as codified until the decision in Kharak Singh v. State of U.P.[12] read into words of Article 21 of the Constitution of India, a Right to Privacy. Thus, Right to Privacy gained a fundamental right status in India and could not be interfered with by the State. It must be noted in this regard that the said decision came subsequent to the decision in State of U.P. v. Raj Narain[13] that gave a fundamental rights status to the right to information. Hence, it is evident that both the decisions are in conflict since right to privacy is antithesis of right to information.

This conflict has now been resolved after a plethora of judgements in this on the subject including the judgement of Mr. 'x' v. Hospital 'Z'[14] wherein the Supreme Court held that Right to Privacy is "not an absolute right and maybe restricted for the prevention of crime, disorder or protection of health or morals or protection on rights and freedom of others". The scope of constitutional Right to Privacy in so far as dissemination of information is concerned, has best been enumerated in Auto Shankar's case wherein it was held, "Right to privacy ... is a right to be let alone. A citizen has a right to safeguard the privacy of his own family, marriage, procreation, motherhood, child bearing and education among other matters. Noone can publish anything concerning the above matters without his consent – whether truthful or otherwise and whether laudatory or critical. If he does so, he would be violating the right to privacy of the person concerned and would be liable in an action in damages". However, this

[11] W.V.H. ROGERS, *WINFIELD AND JOLOWICZ ON TORT* 406–07 (18th ed. 2010) ("There is no general right to privacy, and no tort of invasion of privacy as such."), *Argyll v. Argyll*, [1967] Ch. 302 (Eng.) (Chancery Division) (granting an injunction to prevent publication of confidential marital communications).
[12] AIR 1963 SC 1295.
[13] AIR 1975 SC 865.
[14] AIR 1995 SC 26

right is a part of Article 21 of the Constitution of India and therefore can be enforced only against the State. Apart from the constitutional right, right to privacy is also embodied under S. 43A and 72 of the Information Technology Act (hereinafter "IT Act").

Case law analysis: Cases before the Puttaswamy Judgement regarding privacy

In the case of **M.P. Sharma V Satish Chandra**, the SC held that privacy could not be considered a fundamental right under the Indian Constitution, narrowly interpreting its relevance only within prescribed statutory regulations. A decade later, in Kharak Singh V State of UP, the Court similarly denied privacy as a fundamental right, asserting that surveillance, even under state regulations, did not infringe upon fundamental rights guaranteed by the Constitution.[15]

Subsequently, in **Govind V State of M.P**. the court upheld the validity of state regulations on the Constitution. It advocated for a case-by-case development of privacy rights due to the absence of legislative enactments, thereby broadening the scope of Article 21.

In **ADM Jabalpur V Shivakant Shukla**, the Court deliberated on the restrictions on personal liberty beyond constitutional and statutory provisions, implicitly acknowledging privacy's inclusion in common law. Justice Khanna underscored that the protection of personal liberty extended beyond statutory laws, including common law principles.

Maneka Gandhi V UOI saw a broader interpretation of Article 21, incorporating the concept of natural law, which encompassed personal liberty and security rights, thus reinforcing privacy within the ambit of Right to Life. In R. Rajagopal V State of TN, the Court elaborated on the development and scope of privacy rights, affirming its implicit nature under Article 21 and extending it to safeguard various personal matters. The case recognized privacy as both an actionable claim and a fundamental right.

Finally, in **People's Union for Civil Liberties V UOI**, the Court extended privacy rights to communications, addressing concerns regarding phone tapping and laying down regulations for intercepting orders. It emphasized the case-specific nature of privacy claims and violations,

[15] *M.P. Sharma v. Satish Chandra*, 1954 SCR 1077, AIR 1954 SC 300 (India) (holding that the Indian Constitution does not explicitly protect a right to privacy and rejecting the application of the U.S. Fourth Amendment doctrine).

establishing guidelines for assessing infringements based on factual circumstances.

In the case of **District Registrar and Collector, Hyderabad & anr. V Canara Bank & anr.,** the court underscored that personal liberty, freedom of expression and freedom of movement paved the way for the recognition of the right to privacy. It affirmed that privacy is inherent to individuals and can only be intruded upon through legislative, administrative, or Judicial provisions.[16]

In **Selvi & ors. V State of Karnataka & ors**., the Court distinguished between physical and mental privacy, linking the right to privacy with Article 20(3) (self-incrimination). It acknowledged the distinction between physical privacy, subject to certain legal limitations, and mental privacy, which protects an individual's private thoughts and choices. This case established techniques such as narcoanalysis and polygraph examinations, if conducted without consent, could violate an individual's mental privacy.[17]

In **Unique Identification Authority of India & anr. V. CBI**, the Court addressed the issue of accessing biometric data compiled by the UIDAI for criminal investigation purposes. It ruled that the UIDAI cannot transfer biometric information to any agency or third party without the written consent of the individual. Furthermore, it mandated that individuals cannot be denied services for lack of an Aadhar number if they are otherwise eligible, and authorities must modify their requirements accordingly.[18]

Constitutional Foundations of the Right to Privacy in India

The Indian Constitution does not expressly mention the right to privacy. Nevertheless, the judiciary has interpreted it as being implicit in Article 21, which guarantees the right to life and personal liberty, and also in Articles 14 and 19. The transformation of privacy from a peripheral concept to a central constitutional right culminated in the Supreme Court's 2017 verdict in Justice K.S. Puttaswamy v. Union of India. Post-Puttaswamy, the constitutional mandate for privacy has influenced laws, regulations, and policies, pushing for more robust data protection

[16] *District Registrar & Collector, Hyderabad & Anr. v. Canara Bank & Anr.*, (2005) 1 SCC 496, ¶¶ 35–36 (India) (discussing the constitutional foundation of the right to privacy under Article 21)
[17] *Selvi & Ors. v. State of Karnataka & Ors.*, (2010) 7 SCC 263, ¶¶ 206–211 (India) (discussing the link between involuntary administration of scientific techniques and the protection against self-incrimination under Article 20(3)).
[18] *Unique Identification Auth. of India & Anr. v. CBI*, (2014) 11 SCC 642 (India) (concerning whether biometric data under the Aadhaar scheme could be shared with investigating agencies).

frameworks and re-examination of state surveillance practices.

Case analysis; Justice K.S. Puttaswamy (retd.) & Anr. V. UOI & Ors.[19]

This landmark case serves as the cornerstone of India's 'Right to privacy' jurisprudence, wherein a nine Judge Bench unanimously affirmed the right to privacy as a fundamental right enshrined within the Constitution of India. The Supreme Court asserted that privacy is integral to the freedoms guaranteed by fundamental rights and is a fundamental aspect of dignity, autonomy and liberty. The case originated from a dispute over the legal validity of the Aadhar database, with the central question being the recognition of the right to privacy as a fundamental right. The state's argument, hinged on previous decisions such as M.P. Sharma case and Kharak Singh cases, which suggested that the Constitution did not expressly safeguard the right to privacy. However, subsequent judgements recognized privacy as fundamental, albeit rendered by benches of lesser stature. Given the significance of the matter and the conflicting precedents, the case was referred to a nine Juge Bench. The Bench unanimously confirmed that the right to privacy is protected as an inherent component of the right to life and personal liberty under Article 21, as well as within the freedoms guaranteed by part III of the Constitution, the Court solidified the status of privacy as a fundamental right. Moreover, this case emphasized the necessity for new legislation on data privacy, expanding the boundaries of privacy in personal realms and put privacy as an inherent value within the legal framework. The creation of Digital Personal Data Protection Act, 2023 is a result of this Judgement.

Summary of the case:

This case was initiated by a petition filed by Justice K.S. Puttaswamy, a retired judge of the Karnataka High Court, concerning the Aadhaar Project led by the UIDAI. The Aadhaar number, a 12-digit identification code issued by UIDAI, was integrated into various welfare schemes to stream line service delivery and curb fraudulent claims, justice Puttaswamy's petition challenged the constitutional validity of the Aadhaar card scheme, and over time, other petitions addressing different aspects of Aadhaar were also brought before the Supreme Court.

In 2015, before a three Judge Bench, concerns were raised regarding the government's collection and use of demographic biometric data, alleging violations of the right to privacy. The Attorney General of India contested the existence of a fundamental right to privacy,

[19] https://privacylibrary.ccgnlud.org/case/justice-ks-puttaswamy-ors-vs-union-of-india-ors

citing precedents from M.P. Sharma and Kharak Singh. Despite acknowledging previous Supreme Court decisions affirming the right to privacy as constitutionally protected, the three Judge Bench noted that these decisions were issued by larger benches and thus a three Judge Bench is not enough for this petition. Consequently, the case was referred to a constitutional bench to review the precedents that have been established, along with the validity of subsequent decisions. On 18 July 2017, a nine Judge Bench was deemed appropriate to resolve the issue Contentions: The Respondents primarily relied on judgements in MP Sharma and Kharak Singh cases, which asserted that the Constitution did not expressly safeguard right to privacy. These judgements were delivered by an eight and a six Judge Bench respectively, leading the Respondents to contend that they held binding authority over subsequent decisions rendered by smaller benches. Furthermore, the Respondents argued that the framers of the Constitution did not intend to elevate the right to privacy to the status of a fundamental right.

Contrarily, the Petitioners contended that the rationales underlying the above two judgements were rooted in principles expounded in A.K. Gopalan case. They argued that the Gopalan case's interpretation of fundamental rights as discrete protections for each provision was invalidated by an eleven-Judge Bench in RC Cooper V. UOI. Consequently, the Petitioners argued that the foundation of the aforementioned decisions were flawed.

They further emphasized that in the seven-Judge Bench ruling of the Maneka Gandhi case, the minority opinion of Justice Subba Rao in Kharak Singh was explicitly endorsed while the majority decision was overturned. Additionally, discussions during the proceedings addressed the extent of the right to privacy. The Petitioners advocated for a multifaceted conception of privacy as an inherent fundamental right, while the Respondents posited that privacy was a nebulous concept, suitable for crystallization only through statutory and common law mechanisms.

The Petitioners posited that the Constitution should be construed in accordance with the Preamble, recognizing privacy as a natural and international human right. In contrast, the Respondents advocated for a narrow interpretation, focusing on the Constitution as the source of fundamental rights, with Parliament as the sole authority empowered to amend them.

The landmark decision was delivered through six distinct opinions, the Supreme Court unequivocally affirmed privacy as an autonomous and indispensable fundamental right under

Article 21 of the Constitution of India. The crux of the ruling delineated an expansive construal of privacy, transcending mere physical encroachment or subsidiary entitlement under Article 21, but encompassing the realms of both body and mind, including decisions, choices, information, and liberty. Privacy was adjudged to be a preeminent entitlement within Part III of the Constitution, possessing enforceable and multifaceted dimensions, the particulars of which were expounded upon in the various opinions.

The Court repudiated the precedents set forth in M.P. Sharma and Kharak Singh to the extent that the latter opined the absence of a fundamental right to privacy. Regarding M.P. Sharma, the Court endorsed its stance on the absence of constitutional limitations akin to the Fourth Amendment of the U.S. Constitution regarding search and seizure laws. Nevertheless, the Court maintained that the Fourth Amendment did not exhaustively delineate privacy, and the lack of a corollary protection in the Indian Constitution did not negate the existence of an inherent right to privacy in India. Consequently, the conclusion in M.P. Sharma was overturned. The Court rebuffed the insular perspective of personal liberty espoused in Kharak Singh, likened by Justice D.Y. Chandrachud to the "silos" approach borrowed from A.K. Gopalan. Observing the obsolescence of compartmentalizing fundamental rights post-Maneka Gandhi, the Court noted an inherent contradiction within the majority opinion of Kharak Singh, as there was no legal justification for nullifying domiciliary visits and police surveillance other than privacy, a right acknowledged in theory but disavowed as part of the Constitution. Additionally, the Court underscored that subsequent decisions affirming the right to privacy were to be interpreted in accordance with the principles enunciated in the Kharak Singh judgment. Moreover, the Court scrutinized the affirmative case for the protection of the right to privacy under the rubric of the right to life, personal liberty, and the freedoms enshrined in Part III of the Constitution. The Bench underscored that privacy was not an e xclusive construct, refuting the Attorney General's contention that privacy must yield to the state's welfare entitlements. Notably, while affirming that privacy was not absolute, the judgment expounded on the standard of judicial review applicable in cases of sta te intrusion into individual privacy. The Court stipulated that the right to privacy could be curtailed only if such intrusion satisfied the tripartite requirements of legality, necessity, and proportionality, with Justice S.K Kaul appending procedural safeguards against abuse of such interference as a fourth prong to the test.

Concurrently, Justice J. Chelameswar opined that the "compelling state interest" standard

should be reserved for privacy claims warranting "strict scrutiny", while other claims should be adjudicated under the just, fair, and reasonable standard under Article 21. The application of the "compelling state interest" standard, according to his judgment, was contingent upon the circumstances of the case. Furthermore, the Court emphasized sexual orientation as an integral facet of privacy and elucidated on the negative and positive aspects thereof, stipulating that the State was not only proscribed from encroaching upon the right but also obligated to proactively safeguard individual privacy. Lastly, the judgment acknowledged informational privacy as an inherent component of the right to privacy. While recognizing the necessity for a data protection statute, the Court entrusted the legislation of such laws to the purview of Parliament.

Impact of the Right to Privacy on the Aadhaar Judgment (2018)

Following the 2017 privacy ruling, a five-judge bench of the Supreme Court delivered its verdict on the constitutional validity of the Aadhaar scheme in 2018. While the 2017 judgment had laid the foundation for the recognition of privacy as a fundamental right, the 2018 Aadhaar judgment tested the application of that right against the government's digital identification project

1. Partially Upheld the Aadhaar Act: The Court upheld the constitutionality of the Aadhaar Act, 2016, but struck down or read down several provisions to ensure that the right to privacy is not disproportionately violated.
2. Reasonable Restrictions on Privacy: Applying the three-fold test from Puttaswamy (2017) legality, legitimate aim, and proportionality—the Court found that Aadhaar met these conditions for welfare schemes but failed in other areas.
3. Metadata Retention: The provision permitting indefinite retention of authentication records was limited to six months to reduce the risk of profiling Compulsion in Schools and Exams: The Court ruled that Aadhaar could not be made mandatory for school admissions or CBSE/NEET exams.
4. Data Protection Emphasis: The Court recognized the need for a robust data protection framework in India, aligning with global norms such as the GDPR. It recommended the enactment of such legislation to prevent misuse of personal data.

In an era where technology has become inseparable from everyday life, the concept of privacy has undergone a profound transformation. The digital age, characterized by rapid advancements in information and communication technologies, has expanded the boundaries of human interaction and information sharing. While these developments have created

unprecedented opportunities for connectivity and innovation, they have also given rise to complex legal and ethical questions surrounding individual privacy.[20]

This research seeks to explore the contours of the right to privacy within the digital age, focusing on its constitutional foundations and the implications of technological advancements. It critically analyzes how courts and legislatures have responded to digital privacy concerns and evaluates the adequacy of existing legal safeguards. The study also examines the tension between privacy rights and competing interests such as national security, law enforcement, and corporate data collection.

Constitutional Dimensions of Privacy in India

The Indian constitutional framework did not explicitly recognize privacy as a fundamental right until the landmark judgment in Justice K.S. Puttaswamy v. Union of India (2017), The judgment draws upon both Indian and comparative jurisprudence, including U.S. cases such as Griswold v. Connecticut and Roe v. Wade. Scholars such as Gautam Bhatia have praised the Puttaswamy verdict for reinforcing liberal constitutionalism and laying the groundwork for future privacy claims in India. However, critics have pointed out that despite the strong theoretical recognition, the practical enforcement of privacy rights remains fragmented and limited.

Technological Threats to Privacy

The digital age has ushered in unprecedented threats to personal privacy through data mining, surveillance technologies, facial recognition, biometric databases, and algorithmic profiling. Shoshana Zuboff's concept of "surveillance capitalism" (2019) details how tech corporations commodify personal data, leading to significant power imbalances.[21] Legal scholars such as Julie E. Cohen argue that privacy is not just an individual right but a social and political condition necessary for democratic citizenship. Her works emphasize the structural dimensions of digital surveillance and how law must adapt to evolving technological norms.
In India, the Aadhaar project and its constitutional implications have attracted extensive

[20] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2019) 1 SCC 1 (India) [Aadhaar judgment] (upholding the Aadhaar Act, 2016, while reading down or striking certain provisions to preserve the right to privacy) (striking down mandatory Aadhaar requirements for school admissions, CBSE, and NEET exams as unconstitutional). P.no: 482-483

[21] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs 2019)

commentary. Critics such as Usha Ramanathan and Reetika Khera have cautioned against the normalization of surveillance and data collection by the state, especially in the absence of a robust data protection law.[22]

Statutory Framework Governing Digital Privacy

India's statutory framework for digital privacy has evolved incrementally, primarily through the Information Technology Act, 2000, and, more recently, the Digital Personal Data Protection Act, 2023. These statutes attempt to regulate the collection, storage, and dissemination of digital personal data by both government and private entities. The Information Technology Act, 2000, was India's first law to address electronic commerce and cybersecurity. Although not explicitly framed as a data protection law, it contains two important provisions:

Section 43A – Holds corporations liable to pay compensation if they fail to implement reasonable security practices and cause wrongful loss to individuals.

Section 72A – Penalizes disclosure of personal information without consent.

Privacy as a Fundamental Right in India

One of the most significant developments in Indian constitutional law is the recognition of the right to privacy as a fundamental right in the landmark case Justice K.S. Puttaswamy v. Union of India (2017). The Supreme Court held that privacy is inherent to life and personal liberty under Article 21 of the Constitution. This unanimous decision overruled earlier judgments (M.P. Sharma and Kharak Singh) and laid the constitutional foundation for digital rights jurisprudence in India. The judgment emphasized autonomy, dignity, and the necessity of privacy in democratic participation.

Inadequate Legal and Regulatory Framework

Despite the constitutional status of privacy, India's statutory and regulatory framework remains underdeveloped. The Information Technology Act, 2000, only partially addresses privacy and data protection concerns, and lacks dedicated provisions for personal data handling, profiling, or surveillance. There is a vacuum in data protection law, which allows state and private entities to collect and process personal data without meaningful oversight or user consent. This has

[22] Usha Ramanathan, Aadhar: A Biometric History of India's 12-Digit Revolution, 49 Econ. & Pol. Wkly. 33 (2014)

enabled widespread data breaches, opaque surveillance, and commercial exploitation of user data.

Emerging Technologies Challenge Traditional Notions of Privacy

Digital technologies, particularly artificial intelligence, facial recognition, big data analytics, and biometric systems, have outpaced legal protections. These technologies enable constant monitoring, data mining, predictive profiling, and behavioral tracking, which fundamentally alter the scope and meaning of privacy. The law has struggled to keep up with innovations like algorithmic decision-making, targeted advertising, and location-based tracking, leaving users vulnerable to manipulation and exclusion without effective legal remedies.

State Surveillance and Lack of Accountability

The Indian state has expanded its surveillance capabilities through initiatives such as Aadhaar, NATGRID, and the Central Monitoring System. The Pegasus spyware scandal demonstrated the state's capacity to infiltrate private communications of citizens, journalists, activists, and political opponents. However, there are no robust legal frameworks ensuring judicial oversight, transparency, or proportionality in surveillance practices. This undermines both constitutional guarantees and public trust in government institutions.

Digital Identity and Privacy Trade-offs

Projects like Aadhaar, DigiLocker, and digital health IDs, while enhancing administrative efficiency, raise serious privacy concerns. They collect sensitive personal data without adequate user control or clarity on data retention, sharing, and deletion. Courts have attempted to impose limitations on Aadhaar usage, especially in private services, but implementation remains inconsistent. The trade-off between digital inclusion and privacy protection is often skewed in favor of the state or corporate interests.

Delayed and Diluted Data Protection Legislation

India's long-awaited data protection law—initially proposed as the Personal Data Protection Bill, 2019, and later reintroduced as the Digital Personal Data Protection Bill, 2023—has been criticized for lacking independence in regulatory oversight and for granting excessive exemptions to the government. These exemptions undermine the core principles of necessity and proportionality emphasized in the Puttaswamy judgment. Unlike the GDPR, which has strong enforcement and accountability mechanisms, India's proposed framework risks

becoming symbolic without meaningful safeguards.

Comparative Legal Insights and Global Standards

Comparative analysis reveals India's shortcomings in aligning with international data protection standards. The European Union's GDPR is widely regarded as a robust legal framework that ensures individual consent, data portability, and accountability. The U.S., though fragmented in its approach, has seen increased judicial protection of digital privacy (e.g., Carpenter v. United States). India's current approach, while inspired by these systems, lacks the enforcement strength and user-centric design needed for effective implementation.

Marginalized Communities Face Disproportionate Privacy Risks

Privacy harms are not equally distributed. Marginalized populations—such as minorities, Dalits, Adivasis, LGBTQ+ individuals, and low-income groups—often face systemic data-driven discrimination. Aadhaar-linked welfare schemes have resulted in denial of benefits due to authentication errors. Surveillance technologies in public housing and policing disproportionately target vulnerable communities. The current legal discourse on privacy rarely centers these intersectional concerns, creating a gap in both scholarship and policy.

Judicial Responses Have Been Limited Post-Puttaswamy

While Puttaswamy created a constitutional mandate, subsequent judicial interventions have lacked consistency and strength. Courts have been hesitant to confront executive overreach or suspend state surveillance projects. The absence of judicial review in data-sharing policies, such as the Aarogya Setu app or the use of facial recognition in law enforcement, reflects a passive judicial approach. This undermines the enforceability of privacy rights and calls for a more proactive judicial posture.

Need for Interdisciplinary and Participatory Approaches

Finally, the study finds that the future of privacy law in India must adopt an interdisciplinary approach that incorporates legal, technological, ethical, and policy perspectives. Public awareness about digital privacy remains low, and policymaking often lacks civil society participation.

CONCLUSION

As a cornerstone of individual freedom, privacy is a concept that is extremely essential for humanity. The right to privacy is rooted in human nature's unalienable rights and has historical relevance. In India, the acknowledgment of the right to privacy went through a transforming journey before being affirmed as a fundamental right by a nine-judge Supreme Court bench in the Justice K.S. Puttaswamy v. Union of India case."

In the contemporary era, dominated by the pervasive influence of social media and the internet, has elevated the significance of privacy. Concerns have arisen due to the extensive storage of private information and the potential misuse of technology, particularly by malevolent actors. While social media creates a platform for global exchange and cooperation, it also exposes to individual privacy due to the extraction and utilisation of personal information.

The ever-evolving digital landscape necessitates a careful balance between privacy protection and technological progress and The 'Digital Personal Data Protection Act 2023' represents a significant step towards maintaining this balance and preserving the essence of personal liberty in the ever-expanding digital landscape. India's acknowledgement of the right to privacy has had a profound impact on data protection rules. The right to privacy highlights the significance of individual liberty, consent, and control over personal data. Because everyone has the right to privacy, extensive data protection frameworks have been built to safeguard personal data against unauthorized access, misuse, and abuse.

RECOMMENDATIONS

Here are some suggestions for improving the right to privacy in India:

- Protect personal data The government should ensure that personal and biometric data is protected and used only for the purpose it was collected for.
- Pass a specific law Some say that the current legal framework is not enough to protect personal privacy rights. A specific law on privacy and data protection is needed.
- Implement security measures Organizations should use encryption and anonymization to protect personal data. Alert people to data breaches Organizations should alert people if there is a data breach and give them access to their personal data.
- Conduct audits Organizations should regularly audit their privacy procedures to

understand what data they collect, how it's used, and where it's stored.

- Balance the right to privacy with the right to know The government should not disclose personal information if it's not related to a public interest or if it would invade someone's privacy.
- Limit state action State action can only limit the right to privacy if it has a legislative mandate, pursues a legitimate state objective, and is proportionate.
- The government should ensure the proper mechanism to protect the personal and biometric data of individuals. It should use the data only for the purpose for which it is being collected and must refrain from using it for any surveillance purposes.