A ES
ISSN: 2096-3246
Volume 58, Issue 01, 2026

OUR DATA, OUR RIGHTS: NAVIGATING PRIVACY ON SOCIAL MEDIA AND OTHER ONLINE PLATFORMS.

Tanay Paul
Research Scholar, Department of Law, Gauhati University

Dr. Karavi Barman
Assistant Professor, Department of Law, Gauhati University

Abstract
Online privacy is often referred to controlling of personal information shared on the internet or other social media platforms. This article illustrates the intersection of privacy rights and online platforms, focusing on India's legal framework, global best practices like GDPR and other emerging challenges. It argues that privacy is a fundamental right essential for independence, democracy and human prosperous in the digital age. This paper analyzes India's Constitutional foundations i.e. Article 21 after the Puttaswamy's judgment, the IT Act, the Digital Personal Data Protection Act and the New Digital Personal Data Protection Rules, 2025 and the Judicial Developments, while exploring threats like data harvesting, surveillance, third party tracking and algorithmic biases. The real world case studies like the Whats App Privacy Policy, Aadhaar Data Leak, Cambridge Analytica Scandal illustrates the prevalent privacy violations in large scale. Certain practical steps like Privacy Settings, Two Factors Authentication and Reliable VPN along with future emerging trends like AI and Deep fakes are discussed to under the growing risk of data theft and how to mitigate such losses. Balancing innovation with fundamental rights remains a critical concern for a developing nation like India with more than half of the population with first time internet users. This article concludes by emphasizing shared responsibility among government, online platforms stakeholders and users to balance innovation with dignity.
Keywords : Digital Privacy, Online Platforms, Data Protection, Surveillance.

Introduction

In the blink of a single generation time, the way we communicate, the way we work and learn and the way even we express our love has moved almost entirely onto digital platforms or online platforms. Right from the morning when we start our day with scrolling the social media app to closing our laptops at night, we leave a trail of data that is harvested, analyzed, and often monetized by corporations, governments or other third party agents.[1] The convenience of these services which we enjoy comes with a hidden cost i.e. the erosion of personal privacy.

The right to privacy, once a vague concept confined to philosophical debates or talk shows, has now been recognized as a fundamental right in many jurisdictions, including India, where the Supreme Court declared it an intrinsic part of the right to life and personal liberty under Article 21

[1] Westin, F. Alan, *Privacy and Freedom, Atheneum* 38 (Six Printings, New York, 1970).

ISSN: 2096-3246
Volume 58, Issue 01, 2026

of the Constitution[2]. Yet, the rapid pace of technological change continually outstrips the ability of laws and regulations to keep up with the changing dimensions. This article seeks to provide a thorough examination of privacy rights on social media and other online platforms, with a particular focus on the Indian context, while also drawing an analysis on global best practices.

The article seeks to explore how an individual can assert their rights over personal data on social media and other online platforms and understand how online platforms threatens privacy of an individual and what are the legal landscape available in India for their breaches. This article also highlights how an individual can overcome the hazards of privacy in any online or social media platforms. The article will also try to find various practical measures to mitigate the risk of online privacy in the present day technology. The author through this paper will also try to illustrate the future way ahead and how to improve and minimize the risk of online hazard to protect one's privacy.

Objectives of the study

- To understand the legal landscape for privacy violations in India.
- To understand the judicial developments of privacy and their implications in framing the data protection laws in India.
- To examine the various Global Benchmarks for data protection.
- To give an overview of how online platforms threaten privacy in the present digital world.
- To recognize the various practical steps to protect our privacy rights in online platforms.
- To understand through real life case studies and to highlight certain future trends and emerging issues.

Why Privacy Matters?

Privacy is often described as the "right to be left alone,"[3] but it is not confined to it, it is far more than that. It is a prerequisite for human prosperous, enabling individuals to develop their personalities or skills, form intimate relationships, and exercise autonomy without undue influence or interference. In the digital realm, privacy serves three core functions.

First, it protects personal autonomy - When individuals know that their online activities can be traced, they may self censor, limiting their freedom of expression and their ability to explore new ideas that deviate from societal norms and culture.[4]

[2] Kailash Rai, *Constitutional Law of India* 170 (Central Law Publications, Allahabad, 2001).
[3] Prashant Iyengar,"Privacy and the Information Technology Act in India" 63-64, *SSRN ELIBRARY (*2009).
[4] Gaurav Goyal and Ravinder Kumar, *The Right to Privacy in India* 13 (Partridge Publication, India, 20th edn, 2016).

Second, privacy safeguards information integrity[5]- Personal data ranging from financial data to health records can be weaponized if it falls into the wrong hands, leading to identity theft, financial loss, or even physical harm.
Third, privacy underpins democratic processes - A society in which citizens fear surveillance is less likely to engage in vigorous political discourse or disagreement, a occurrence that has been recognized in authoritarian regimes worldwide.[6]

The stakes are especially high in the Indian context, where a large proportion of the population is using social media or purchasing from online platforms for the first time. According to the Internet and Mobile Association of India (IAMAI), India had over 886 million internet users as of 2024[7]. This number of users will increase rapidly but the first generation internet users are often unaware that the data they are sharing are making them vulnerable to exploitation.

Moreover, the recent COVID-19 pandemic accelerated the shift to new online services like work from home, online shopping of medicine or groceries and online education making privacy concerns more pressing than ever. The pandemic demonstrated how quickly personal data could be repurposed, from contact tracing apps to vaccine distribution websites, often with very little transparency or oversight.[8] In short, privacy is not a luxury but a fundamental pillar of a free and democratic society. Protecting it also on online platforms is therefore not merely a technical issue but a societal imperative.

The Legal Landscape in India

Constitutional Foundations

The Indian Constitution does not explicitly mention the word "privacy," but the Supreme Court has interpreted the right to privacy as part of Article 21, which guarantees the right to life and personal liberty. The landmark judgment in Justice K.S. Puttaswamy (Retd.) v. Union of India[9] affirmed that privacy is a fundamental right, subject to reasonable restrictions imposed by law. This decision laid the groundwork for subsequent data protection legislation in India.

The Information Technology Act, 2000

The primary legislation governing any cyber activities in India is the Information Technology (IT) Act, 2000, along with its accompanying sub clauses and rules. Section 43A[10] of the Act imposes

[5] *Ibid.*
[6] *Ibid.*
[7] https://indianexpress.com (last visited on November 27, 2024).
[8] Mohamad Ayb Dar and Shahnawaz Ahmad Wani," COVID-19, Personal Data Protection and Privacy in India", 15 Asian BioethicsReview, 126 (2023).
[9] AIR 2017 SC4161.
[10] Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any

liability on corporations that fail to protect sensitive personal data, while the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (often referred to as the SPDI Rules) set out baseline standards for data protection in India. However, these rules are limited in scope, applying only to "sensitive personal data"[11] and lacking a comprehensive enforcement mechanism.

The Digital Personal Data Protection Act, 2023

In response to growing concerns, the Indian government introduced the Personal Data Protection Bill (PDPB) in 2019 and subsequently the India's Digital Personal Data Protection (DPDP) Act, 2023 was enacted in August, 2023. The Act mainly seeks to create a comprehensive data protection framework law to protect digital personal data and supervision. Its key provisions include-

(a) Consent - Data fiduciaries must obtain clear, informed consent from data principals before processing personal data for any use.

(b) Purpose Limitation - Data can only be used for the specific purpose for which it was collected and not for any other subsidiary use.

(c) Data Localization - Certain categories of sensitive personal data must be stored only on servers located within India.

(d) Right to be Forgotten - Data principals can request the deletion of their personal data under certain conditions.

(e) Data Protection Authority (DPA) - An independent regulatory authority would oversee any grievance or compliance, impose penalties, and issue guidelines for any violations.

While the DPDP Act, 2023 represents a significant step forward yet it has faced criticism for granting the government broad exemptions, particularly for "national security" and "public order."[12]

person, such body corporate shall be liable to pay damages by way of compensation to the person so affected. *Explanation* - For the purposes of this section, -

(i) "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;

(ii) "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;

(iii) "sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

[11] *Id.* at 3.

[12] M.L.Upadhyaya and P.Jayaswal,"Constitutional Control of Right to Privacy" 2 *CILQ* 39(1989).

ISSN: 2096-3246
Volume 58, Issue 01, 2026

Judicial Developments in India

Judicial development in privacy cases has really accelerated its speed over the past decade. First off was the 2017 Justice K.S. Puttaswamy (Retd.) v. Union of India[13], where a nine judge bench declared that privacy is a fundamental right under Article 21 of the Constitution of India. That ruling not only overturned earlier judgments that had treated privacy as a mere "penumbra"[14] but also set the proportionality test that any state intrusion must be lawful, necessary and not arbitrary. Since then, the courts have been busy fleshing out what that right looks like in present day practice. The Bombay High Court's 2019 Vineet Kumar v. CBI[15] judgment struck down illegal phone tapping orders, emphasizing procedural safeguards. In 2022, the Delhi High Court's Jorawar Singh Mundy case[16] ordered online legal databases to scrub a judgment that exposed a petitioner's name, showing how privacy can even trump the public's right to information .

Fast forward to July 2024, the Supreme Court doubled down in K.S. Puttaswamy (Retd.) v. Union of India[17] explicitly recognizing data privacy as a distinct fundamental right and laying down a detailed framework consent, purpose limitation, security safeguards, etc. that mirrors the GDPR's principles .[18] This judgment gave the much awaited the Digital Personal Data Protection (DPDP) Act a solid constitutional backing.

All of these judicial developments show a clear pathway that judiciary has moved from recognizing privacy as an theoretical liberty to spelling out concrete rights and obligations for both the state and private players. The next few years will be about how well the new DPDP framework holds up under the proportionality test laid down in Puttaswamy case and whether the courts continue to expand the "right to be forgotten" and other facets of informational privacy rights.

So, in a nutshell, we've gone from a landmark constitutional pronouncement to a full blown data protection regime, with the courts playing the role of both guardian and interpreter every step of the way. These cases illustrate a judicial willingness to protect privacy, even as they navigate the tension between security and individual rights.[19]

Global Benchmarks: The GDPR and Beyond

The European Union's General Data Protection Regulation (GDPR), which came into force in 2018, is widely regarded as the gold standard for data protection. Its core principles—lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation,

[13] AIR 2017 SC4161.
[14] *Id.* at 12.
[15] SLP (Criminal) 902/2020.
[16] W.P.(C) 3918/2021.
[17] Writ Petition (Civil) No. 123 of 2024.
[18] *Id.* at 12.
[19] Charles and Louis D Brandies, "The Right to Privacy" 4 *HLR* 18 (1969).

integrity, and confidentiality have influenced privacy laws worldwide, including India's PDPB or DPDP Act or the new DPDP Rules,2025[20].

Key GDPR concepts that have resonated globally include-
(a) Consent - Must be freely given i.e. free consent, specific, informed, and unambiguous.
(b) Data Subject Rights - Individuals have rights to access, fix, erase, restrict processing, and data portability.
(c) Privacy Impact Assessments (PIAs) - Organizations must assess the impact of processing operations on privacy.
(d) Breach Notification - Controllers must notify the relevant supervisory authority within 72 hours of a breach.

While the GDPR's extraterritorial reach means that many Indian companies serving EU citizens must comply the regulation and it serves as a benchmark for best practices that can be adopted domestically.

Other jurisdictions such as California's Consumer Privacy Act (CCPA), Brazil's Lei Geral de Protecao de Dados (LGPD), and Australia's Privacy Act offer additional models[21]. However, the GDPR remains the most exhaustive and comprehensive, and its influence is evident in the drafting of the PDPB in India.

How Online Platforms Threaten Privacy

(a) Data Collection Practices

Online platforms collect data at every step when we create an account, when we like or comment on a post, when we search for a product, and even when we simply scroll over any online news feed. This data is aggregated into comprehensive profiles that can reveal various intimate aspects of a person's life, political beliefs, health conditions, sexual orientation, and financial status.

(b) Third Party Tracking

Cookies, pixels, and SDKs embedded in apps allow third parties advertisers, analytics providers, and even data brokers to track users across multiple sites and devices. This "shadow profiling"[22] often occurs without the user's knowledge or free consent, creating a surveillance ecosystem that is difficult to escape in this digital age.

(c) Algorithmic Decision Making

[20] *Supra* note 5 at 16-18.
[21] Alibeigi Ali, Abu Bakar Munir, *et.al.*,"Right to Privacy, a Complicated Concept to Review",*Library Philosophy and Practice (*e-article) 25(2019).
[22] http://en.m.wikipedia.org/wiki/privacy-laws(last visited on December 01,2025).

Machine learning algorithms use the collected and encrypted data to make predictions about users determining what content they see, what ads to be shown, and even what job opportunities to be offered.[23] While these systems can be highly efficient and effective, they can also be responsible for biases, leading to discriminatory outcomes. The cloudiness of these algorithms raises serious accountability concerns.

(d) Data Breaches

High profile breaches such as the 2018 Facebook Cambridge Analytica scandal, which exposed the data of up to 87 million Facebook users demonstrate the real world consequences of inadequate security in the digital platforms. In India, the 2020 leak of 1.6 million Aadhaar records highlighted the vulnerability of even government run databases.[24]

(e) Government Surveillance

In some cases, governments compel online platforms to hand over user sensitive data, often citing national security or law enforcement reasons. The lack of transparent oversight mechanisms can lead to abuse, as seen in the 2021 Pegasus spyware controversy, where journalists and activists in India were allegedly targeted.

(f) Emerging Technologies

The rise of the Internet of Things, facial recognition systems, smart watches and other wearables adds new dimensions to privacy risk. Devices that continuously monitor the user's location, biometric data, or even heart rate can generate highly sensitive information and if it is mishandled they could have far reaching implications.[25]

Practical Steps to Protect Our Privacy

While the responsibility for online privacy cannot rest solely on individuals, there are several steps users can take to mitigate risk. Some of the precautionary measures that can be adopted are as follows-

1. Review Privacy Settings - Most online platforms offer granular controls over who can see their posts or profile, what data is shared with third parties, and how one's activity is tracked. Every individual must take the time and precaution to adjust these privacy settings rather than accepting defaults.

2. Use Strong, Unique Passwords - A password manager can generate and store complex and unique passwords, reducing the risk of credential hacking and cyber attacks.

[23] *Ibid.*
[24] P.Goffman, Samuel D. Warren and Lois Brandies," The Right to privacy" 4 Harvard Law Review, 27 (1980).
[25] *Supra* note 12.

3. Enable Two Factor Authentication (2FA) - 2FA adds an extra layer of security for any online platforms, making it harder for hackers to gain unauthorized access.

4. Limit App Permissions – Every individual must regularly review the privacy permissions granted to mobile apps particularly those that request access to the camera, microphone, location, or contacts.

5. Use a Reliable VPN - A virtual private network encrypts our internet traffic, masking our IP address and protecting data from eavesdropping on public or unreliable Wi-Fi networks.

6. Be Cautious with Personal Information – One must avoid sharing sensitive or personal details such as complete date of birth, full address, or other financial information unless absolutely necessary.

7. Opt Out of Data Sharing Programs[26] - Many online platforms provide mechanisms to opt out of targeted advertising or data sharing with third parties and one must block such unwanted advertising or cookies.

8. Regularly Monitor Account Activity - Keep an eye on every login history, transaction records, and unusual activity. Every user must promptly report any such suspicious behavior and take immediate action.

9. Use Privacy Focused Browsers and Extensions - Browsers like Brave or Firefox, combined with extensions such as uBlock Origin and HTTPS Everywhere, can block trackers and enforce secure connections.[27]

10. Stay Informed - Privacy laws and online platform policies evolve with the changing times. Following reputable tech news outlets and privacy advocacy groups can help one stay ahead of new threats.

These measures or precautions are not foolproof security, but they significantly reduce the risk of attack and value our privacy.

Case Studies: Privacy in Action

(a)The WhatsApp Privacy Policy Controversy (2021)

In early 2021, WhatsApp updated its privacy policy to require users to share more data with its parent company, Facebook. The move sparked a massive backlash in India, with users migrating

[26] S.k.Verma and Raman Mittal (eds.), *Legal Dimensions of Cyber Space*(ILI,Delhi,2021).
[27] *Ibid.*

to alternatives such as Signal and Telegram. The incident highlighted the power imbalance between platform owners and users, as well as the importance of clear, transparent communication about data use.[28]

(b) Aadhaar Data Leak (2020)
A security researcher discovered that a government portal exposing Aadhaar numbers and other personal details of over a billion Indians was left unprotected. The incident led to public outrage and calls for stricter data protection laws[29]. While the government later secured the portal, the breach underscored the risks of centralized databases and the need for robust security practices, even for state run initiatives.

(c) The Cambridge Analytica Scandal (2018)
Although a global story, the scandal had significant repercussions in India, where political parties were alleged to have used harvested data to micro target voters. The episode prompted the Indian government to scrutinize foreign data processing firms operating in the country and reinforced the case for a domestic data protection framework.[30]

(d) Facial Recognition in Retail (2022)
A major Indian retailer piloted a facial recognition system to analyze customer demographics and optimize store layouts. While the technology promised improved customer experience, privacy advocates raised concerns about consent, data storage, and the potential for misuse. The pilot was eventually discontinued after public pressure and regulatory scrutiny.[31]

These cases illustrate the delicate balance between innovation and privacy, and the pivotal role that public opinion, media coverage, and legal intervention can play in shaping outcomes.

The Road Ahead: Future Trends and Emerging Issues
(a)Implementation of the DPDP Act.
The DPDP Act is expected to undergo further amendments with New Digital Personal Data Protection Rules, 2025. Key points of debate include the scope of government exemptions, the independence of the DPA, and the enforcement of data localization requirements. The outcome will determine whether India adopts a GDPR style regime or a more hybrid model that accommodates its unique socio-economic context.

(b) Rise of Decentralized Technologies

[28] Samarth Krishnan Luthra and Vasundhara Bakhru,"Publicity Rights and the Right to Privacy in India" *National Law School of India Review* 131 (2019).
[29] *Ibid.*
[30] *Ibid.*
[31] *Id.*

Block chain and decentralized identity solutions offer the promise of user controlled data, where individuals hold cryptographic keys to their information rather than relying on centralized custodians. While still in early stages, these technologies could reshape the privacy paradigm by reducing the risk of mass data breaches.

(c) AI Generated Deepfakes
Advances in generative AI make it possible to create highly realistic deepfake videos and audio recordings. The potential for misuse such as defamation, blackmail, or political manipulation poses a new challenge for privacy and legal systems. Policymakers will need to grapple with questions of consent, attribution, and platform liability.

(d) Biometric Authentication
Biometric data fingerprints, iris scans, voiceprints are increasingly used for authentication on smart phones and financial apps. While convenient, the irreversible nature of biometric identifiers means that a breach could have lifelong consequences. Future regulations may impose stricter standards for storage, encryption, and usage of biometric data.

(e) Global Data Governance
As data flows across borders, there is a growing push for international standards. Initiatives such as the Digital Geneva Convention and the UN's Draft Resolution on Privacy in the Digital Age aim to establish norms for cross border data sharing, surveillance, and human rights protections. India's participation in these discussions will influence its own regulatory trajectory.

(f) Privacy as a Competitive Advantage
Companies that prioritize privacy by design and default are increasingly seeing a market advantage. Apple's "Privacy First"[32] branding has resonated with consumers wary of data exploitation. In the Indian market, businesses that can demonstrate compliance with emerging privacy standards may differentiate themselves and build trust with users.

Findings of the Study
The researcher have thoroughly and extensively studied the various Constitutional provisions, Information Technology Act 2000, SPDI Rules, 2011, Digital Personal Data Protection Act,2023 and the New Digital Personal Data Protection Rules,2025 and what is seen that these laws are not enough to curb the digital privacy in today emerging technological world. The DPDP Act's government exemptions for surveillance in the name of national security may weaken the very core foundation of privacy. The most vulnerable group i.e. children and their personal data in case of online privacy in not properly addressed. The DPDP Act tried to cater to this problem by

[32] Abisha Isaac George,"Right to Privacy and Freedom of Speech in WhatsApp Group: A Critical Overview" 6 IMadras Law Journal, 5(2023).

obtaining verifiable parental consent before processing children's data and is prohibited from using such data for specific purposes like targeted advertising but how consent should be obtained including requirements for verified identity and age verification is silent. The rapidly changing AI Technology, Deep Fakes, misinformation and other technology data breach on social media or other online platforms is not properly addressed. The researcher found out that the general public especially the first generation users must be made aware about the various protection available and it must be made clearly visible in all online platforms and the remedy available in case of any breaches.

Conclusion

Privacy rights on online platforms are at a crossroads. The digital revolution has delivered unprecedented connectivity, but it has also exposed individuals to new forms of surveillance, exploitation, and discrimination. In India, the constitutional recognition of privacy, coupled with evolving legislation such as the DPDP Act, signals a commitment to safeguarding personal data. Yet, the gap between law on paper and practice on the ground remains wide, especially as technology continues to evolve at breakneck speed.

The responsibility for protecting privacy is shared among governments, platform operators, and users themselves. Policymakers must craft clear, enforceable rules that balance security, innovation, and fundamental rights. Platforms need to adopt privacy by design principles, be transparent about data practices, and invest in robust security measures. Users, meanwhile, must become more vigilant, informed, and proactive in managing their digital footprints.