Sarcouncil Journal of Arts Humanities and Social Sciences

ISSN(Online): 2945-3488

Volume- 04| Issue- 08| 2025

Research Article **Received:** 15-07-2025 | **Accepted:** 10-08-2025 | **Published:** 25-08-2025

Increasing Threat to the Right to Privacy in Digital Age: An Overview

Dr. Ashwani kumar

Principal, Himachal Pradesh College of Law, Kala- Amb, sirmaur, H.P

Abstract: Technological advancements have significantly improved the quality of human life. However, as digital technologies continue to evolve, they have begun to pose serious challenges to individual freedoms. One of the most pressing concerns in this digital era is the right to privacy, especially as personal data is constantly collected, stored, and utilized across various sectors. The rapid digitization of services has also led to the emergence of various cybercrimes, including identity theft, fraudulent communications, cyberstalking, and more. Personal data shared on digital platforms—whether for social networking, commercial transactions, analytics, or governmental use—is often vulnerable to misuse. This raises serious questions about data security and the ethical handling of information. Currently, there is a notable absence of comprehensive legislation in India specifically regulating the collection, storage, monitoring, retrieval, processing, dissemination, and protection of user data. This paper aims to critically examine the evolving challenges associated with the right to privacy and data governance in the digital age. It approaches the issue from two distinct angles: first, by assessing the state's expanding capacity for surveillance; and second, by evaluating consumer privacy concerns, particularly in relation to protections offered under the Competition Act, 2002. The paper concludes by drawing insights from international practices and judicial precedents, offering guidance on how India might better structure its privacy and data protection framework in the future.

Keywords: Right to privacy, digital era, data, user.

INTRODUCTION

The concept of the right to privacy encompasses a range of dimensions. In the context of the digital world, it refers to an individual's ability to exercise control over the collection, storage, and sharing of their personally identifiable information. This personal data includes a wide variety of details—such as a person's identity, interests, habits, education, financial and health records, and even data about those they interact with. Such information, when misused, can be exploited for multiple purposes, including surveillance by the state or for commercial advantages by private entities.

Although the Constitution of India does not explicitly enumerate the "right to privacy" as a fundamental right, this changed significantly with a landmark judgment in August 2017, when the Supreme Court declared it a fundamental right under the Constitution. Despite this judicial recognition, India still lacks comprehensive data protection legislation or a dedicated statutory authority to oversee data privacy enforcement. Nonetheless, substantial progress has been made toward acknowledging and securing the individual's right to privacy.

Historically, in ***M.P. Sharma v. Satish Chandra,*** the Supreme Court ruled that the Constitution did not explicitly guarantee a right to privacy. The case revolved around whether a search order under Section 96(1) of the Criminal Procedure Code violated Article 19(1)(f). In another notable case, ***Kharak Singh v. State of Uttar Pradesh,*** the Court took a different view. Here, it examined the constitutionality of constant police surveillance as per U.P. Police Regulations. Though the petitioner was acquitted of dacoity charges, the Court discussed whether such surveillance infringed upon rights protected under Articles 21 and 19(1)(d), thereby hinting at privacy being an implicit constitutional right.

As jurisprudence evolved, the Supreme Court broadened its interpretation of privacy to include aspects of family life, home affairs, and personal matters—although subject to "compelling state interest." While addressing the legality of telephone tapping, the Court found that intercepting telecommunication without consent constituted a serious invasion of privacy. It also began to distinguish between physical privacy and mental privacy as distinct but interconnected concepts.

In the case of ***Unique Identification Authority of India v. Central Bureau of Investigation,*** the Court held that biometric data linked to Aadhaar cannot be shared with third parties without explicit consent, highlighting the importance of protecting sensitive personal information.

The pivotal moment came in ***K.S. Puttaswamy v. Union of India,*** which challenged the Aadhaar-based Unique Identity Scheme on grounds of privacy infringement. With no specific provision

***Corresponding Author:** Dr. Ashwani kumar

DOI- https://doi.org/10.5281/zenodo.21545819

in the Constitution explicitly laying out the right to privacy, the nine-judge constitutional bench undertook the task of determining whether such a right was protected implicitly. The Court unanimously ruled that privacy is a constitutionally protected fundamental right, stemming from Article 21, among others. The judgment set a new precedent by delving deeply into the nature of privacy, examining global privacy laws, and acknowledging the increasing role of data in both state governance and commercial operations.

Prior to this recognition, some limited safeguards were present in Section 43-A and 72-A of the Information Technology Act, 2000, which offered partial protection of personal data. The Indian Telegraph Act, 1885, also regulated the interception of communications to an extent. More recently, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 have mandated stricter accountability for digital platforms collecting user data, emphasizing the protection of individual privacy in the online domain.

RIGHT TO PRIVACY CONFLICTING WITH STATE INTERESTS

End-to-End Encryption (E2E) ensures that messages sent between a sender and recipient remain unintelligible to anyone—including the network, service provider, or third parties—by encrypting data at the point of origin and decrypting it only at the destination. A unique encryption key is used, preventing tampering or interception during transmission. In an always-online world, E2E protects users' communication footprints across the internet.

In this context, Ruth Gavison's "limited access theory" resonates: privacy concerns focus on who can access our data and to what extent. In a world where smartphones serve as digital diaries of our lives, exposure of personal information can have severe implications.

E2E is especially vital for those in vulnerable or high-risk professions—such as investigative journalists, human rights defenders, activists, civil society leaders, or marginalized communities subject to persecution. It safeguards the right to free speech and association, as guaranteed under Article 19(1)(a) and 19(1)(b). By protecting communication from interception, E2E helps preserve the freedom of peaceful assembly and association. Conversely, nations like Iran, which have restricted encryption tools, have effectively curtailed public mobilisation by significantly degrading encrypted communications during protest periods, limiting planning and coordination.

Still, the Indian Constitution allows reasonable restrictions under Article 19(2)—including for national security. The landmark K.S. Puttaswamy judgment further established a rigorous test to assess whether any limitation on privacy or expression is constitutional. Any restriction must satisfy:

- Be prescribed by law
- Serve a legitimate state interest
- Be proportional, meaning
- It is a suitable method
- There are no less restrictive alternatives
- It does not disproportionately infringe on rights

Restrictions that fail any of these criteria would amount to unconstitutional violations of fundamental rights.

While Section 84A of the Information Technology (Amendment) Act, 2008 allows the government to frame encryption policy, a 2015 draft proposal to dilute encryption standards faced public backlash and was withdrawn—largely due to concerns that it undermined both privacy and free expression.

There is a delicate trade-off between safeguarding public interest and preserving digital rights. Overly rigid encryption regulations or mandatory decrypt access could, paradoxically, weaken national security—by eliminating channels that enable secure reporting, dissent, or whistleblowing. For instance, after the 26/11 attacks, the Indian government pressed Blackberry's parent company to localize data to aid in investigations. Similarly, the Reserve Bank of India mandated local data storage for payment systems in 2018 to reduce fraud risk.

The IT Rules (2021) create a dilemma for communication platforms: to retain safe harbour protection, intermediaries must comply with state data requests within 72 hours—and refusal may expose them to liability. With no explicit limitations on the type of data that can be demanded, intermediaries face a choice: retain encryption integrity or risk losing legal protection under safe-harbour provisions.

Further, the Ministry of Home Affairs (2018) granted ten agencies expansive powers to intercept, monitor, and decrypt communications.

Publisher: SARC Publisher

Such powers must still conform to the Puttaswamy proportionality framework, which these broad surveillance authorisations arguably do not satisfy.

COVID-19 contact tracing apps also raise privacy concerns—centralized models store device data on government servers; decentralized ones store it locally until required. In both cases, user privacy can be jeopardized depending on architecture and access protocols.

On the international front, India's accession to the Five Eyes Intelligence Alliance in October 2020 reignited debates around "backdoors"—government-mandated access to encrypted systems. As former U.S. President Obama warned, backdoors should be implemented only if the benefits substantially outweigh the risks. Historical instances like the 2005 "Athens Affair"—where Greece's public officials were under surveillance via a crypto backdoor—demonstrate how such mechanisms can be misused by foreign or domestic actors, undermining the very privacy they were meant to protect.

THE EVOLUTION OF RIGHT TO PRIVACY IN INDIA

In the 21st century, privacy has emerged as one of the most contested and significant rights, especially in societies undergoing rapid digital transformation. With smartphones, artificial intelligence, and cloud-based ecosystems becoming integral to daily life, citizens leave behind digital footprints at an unprecedented rate. In a country like India, with over 800 million internet users (Internet and Mobile Association of India [IAMAI], 2023), the management, collection, and dissemination of personal data have brought privacy into the centre stage of legal, ethical, and policy debates.

While the Indian Constitution does not explicitly mention the "right to privacy," judicial interpretation has progressively broadened the scope of Article 21 (Right to Life and Personal Liberty) to include this crucial liberty. The Supreme Court's 2017 ruling in ***K.S. Puttaswamy v. Union of India*** recognized privacy as an intrinsic part of human dignity and autonomy (Supreme Court of India, 2017). However, significant gaps persist in law, regulation, and enforcement mechanisms. This paper critically analyzes these challenges across legislative, technological, economic, and institutional domains.

Judicial Trajectory

The recognition of privacy as a constitutional right in India has evolved through several landmark judgments:

M.P. Sharma v. Satish Chandra (1954) – The Supreme Court held that the Indian Constitution did not confer a right to privacy as fundamental (Supreme Court of India, 1954).

Kharak Singh v. State of U.P. (1962) – A partial acknowledgment was made, with the court striking down intrusive police regulations but not categorically recognizing privacy (Supreme Court of India, 1962).

Gobind v. State of M.P. (1975) – The court acknowledged that privacy could be a fundamental right, but only when balanced against compelling state interests (Supreme Court of India, 1975).

K.S. Puttaswamy v. Union of India (2017) – This nine-judge bench conclusively recognized privacy as a constitutionally protected fundamental right under Article 21 (Supreme Court of India, 2017).

Legislative Developments

While the judiciary recognized the right to privacy, legislation lagged behind. India's regulatory framework remained fragmented across acts like:

-The Information Technology Act, 2000 (Government of India, 2000).
-Indian Telegraph Act, 1885 (Government of India, 1885).
-UIDAI Guidelines (Aadhaar).

The Personal Data Protection Bill, introduced in 2019 and withdrawn in 2022, marked an attempt at comprehensive reform but drew criticism for its excessive exemptions to government agencies (Ministry of Electronics and Information Technology, 2019).

Contemporary Challenges

a) Absence of a Robust Legal Framework

India lacks an umbrella legislation akin to the EU's General Data Protection Regulation (GDPR). Though the Digital Personal Data Protection Act, 2023 was introduced with positive intent, concerns remain:

b) Vague Definitions: Key terms like "public interest" or "national security" are not well-defined.

c) Exemptions for Government: The act grants sweeping powers to the government to exempt any of its departments from data protection obligations (Government of India, 2023).

Publisher: SARC Publisher

d) Weak Enforcement: Absence of a strong and independent Data Protection Authority.

e) Rise of Surveillance State

The Indian state's increasing reliance on mass surveillance has raised significant privacy concerns:

f) Aadhaar Project: Although the Puttaswamy judgment upheld its validity, questions linger over biometric data storage and misuse (Supreme Court of India, 2018).

g) Facial Recognition Systems: Deployed in public spaces without informed consent (Internet Freedom Foundation, 2021).

h) Central Monitoring System (CMS) and NATGRID: Enable extensive surveillance of digital and telephonic communication, often bypassing judicial oversight (Software Freedom Law Centre, 2020).

i) Private Sector Exploitation of Data

Corporations often collect, process, and monetize personal data with limited account. Users consent to data use via ambiguous "Terms of Service." Many services are free but extract vast volumes of personal data for targeted advertising, profiling, and predictive analysis (Srikrishna Committee Report, 2018). Big Tech firms like Google, Amazon, and Meta dominate user data, creating anti-competitive environments. Technologies like Artificial Intelligence, Blockchain, and Internet of Things (IoT) complicate privacy governance. Users often don't know how their data is processed or stored. Even anonymized datasets can be reverse-engineered to identify individuals (Narayanan & Shmatikov, 2008). Cross-border data flows challenge jurisdiction and enforcement. The intersection between data privacy and competition is becoming critical in the digital economy. Entities with access to unique datasets create entry barriers for new firms (Organisation for Economic Co-operation and Development [OECD], 2020). Traditional antitrust models focus on pricing; modern privacy breaches inflict non-monetary harms like manipulation or emotional distress (Stucke & Grunes, 2016).

Case Studies

a) Cambridge Analytica Scandal – Exploitation of Facebook user data for political manipulation (Cadwalladr & Graham-Harrison, 2018).

b) Amazon Price Test – Use of user data for algorithmic price discrimination.

Lessons for India

-Establish an independent Data Protection Authority.

-Balance innovation with rights by encouraging Privacy by Design.

-Ensure data minimization and purpose limitation.

-Introduce digital literacy as a civic responsibility.

-Data Localization and Sovereignty

-A rising trend globally and in India is the emphasis on data localization – the requirement that personal data be stored within national borders. This is driven by:

a)National Security Concerns

b)Regulatory Oversight

c) Economic Benefits

However, critics argue it may:

-Disrupt Global Trade

-Increase Compliance Costs

-Stifle Innovation

-India's Competition Commission must update its analytical tools to incorporate data-driven market dominance.

-Comparative Analysis with Global Norms

-European Union – GDPR Model

-User-Centric Approach: Right to be forgotten, data portability, and explicit consent (European Union, 2016).

-Strong Enforcement: Data Protection Authorities with significant autonomy.

-High Penalties: Non-compliance invites severe fines.

-United States – Sectoral Model

-Privacy governed by a web of sector-specific laws (e.g., HIPAA, COPPA). Federal Trade Commission enforces consumer protection but lacks overarching privacy authority (Solove & Schwartz, 2020). So, a balanced localization policy with clear rules on cross-border transfers is essential.

EMERGING THREATS

a) Deepfakes and Synthetic Media: Pose risks of impersonation, identity theft, and misinformation. Growing use of ed-tech and entertainment platforms among minors makes them vulnerable (UNICEF, 2021). Frequent leaks from both public and private databases erode public trust (Indian Computer Emergency Response Team [CERT-IN], 2022). Many citizens are unaware of their digital rights.

b) Overlapping Jurisdictions: Multiple agencies (UIDAI, MeitY, TRAI) create regulatory confusion.

c) Digital Divide: Rural and marginalized communities face greater vulnerability due to limited digital literacy.

Publisher: SARC Publisher

d) State-Citizen Power Asymmetry: Individuals often lack the means to contest surveillance or data misuse.

THREAT TO DATA UNDER COMPETITION LAW

The interaction between businesses and consumers is undergoing a significant transformation due to the rapid expansion of the digital economy—a term that refers to market ecosystems powered by computer-based technologies for the exchange of goods and services. In this evolving landscape, information has emerged as a key commodity. The collection and analysis of consumer data is now central to business strategies, enabling companies to tailor their offerings more precisely and predict customer behaviour.

In effect, personal data has become the new currency of digital marketplaces. By mining data such as preferences, habits, and transactional histories, companies can create demand rather than merely respond to it, thereby circumventing the conventional supply-demand model. However, this raises two critical concerns:

- The erosion of individual privacy and autonomy.
- A growing inequality between companies that possess vast data reservoirs and those that do not.

These issues have attracted the attention of competition law regulators, since antitrust frameworks aim to ensure economic fairness, consumer welfare, and prevent market monopolization. Yet, traditional antitrust scrutiny has focused largely on pricing models—how companies set and vary prices. The use of data, being a non-pricing competitive factor, often escapes regulatory attention despite having profound implications on market dynamics.

An example of this is Amazon's "Price Test" experiment in the early 2000s. The company used historical consumer data to predict the highest price consumers might tolerate for DVDs. This kind of first-degree price discrimination, made possible by detailed data analysis, stirred public backlash and was ultimately shelved. Nonetheless, it demonstrated how data could be exploited to extract maximum value from consumers, potentially at the cost of consumer welfare.

Similarly, Uber leverages data on user movement patterns—tracking when and where users travel, dine, or work out. Voice-activated devices like Amazon Echo and Google Home are constantly listening for wake words, raising concerns about passive surveillance. The infamous Cambridge Analytica incident—where data from approximately 87 million Facebook profiles was harvested for political manipulation during the 2016 U.S. election—further highlights the risks of unchecked data exploitation.

These practices raise critical privacy issues, particularly because many jurisdictions, including India, still lack robust data protection frameworks. Companies often include data-sharing permissions in long, opaque user agreements, leaving users with little real choice or understanding—a phenomenon that undermines the notion of informed consent.

From a competition standpoint, the dominance of major tech companies presents another challenge. Smaller businesses or new entrants often lack access to the volume or quality of user data needed to compete. This creates barriers to entry, particularly when dominant firms possess unique and non-replicable datasets. As a result, the digital economy risks evolving into a "winner-takes-all" model, where the largest players continually consolidate their advantage.

Mergers and acquisitions further reinforce this imbalance. When data-rich firms combine, they aggregate even larger troves of personal data, which can strengthen their market dominance. For instance:
Google's acquisition of DoubleClick expanded its advertising capabilities through enhanced user tracking. Microsoft's merger with LinkedIn allowed for deeper integration between its communication tools and a vast professional network.

The European Commission (EC) has noted that such combinations can significantly boost user reach and potentially distort market competition. In the case of LinkedIn merging with Outlook.com, the EC warned that LinkedIn could gain an undue strategic advantage, limiting opportunities for rivals.

Antitrust bodies assess such mergers by weighing their potential benefits against possible harms. If the combined datasets grant the merged entity a powerful, hard-to-replicate advantage, regulators may impose conditions or block the merger altogether. The competitive landscape and availability of similar data elsewhere are critical factors in this assessment.

Publisher: SARC Publisher

Notably, the EC has clarified that it's not necessarily anti-competitive for a dominant firm to refuse access to its data. However, if the data in question is essential for effective competition and cannot be reasonably sourced elsewhere, denial of access could be deemed an abuse of dominance. In such cases, challengers must prove the uniqueness and indispensability of the data.

RECOMMENDATIONS TO COMBAT THE SITUATION

-Enact a Comprehensive Data Protection Law
-Include clear definitions and narrow exemptions.
-Empower a truly independent Data Protection Authority.

Judicial Oversight for Surveillance
-All surveillance requests should require judicial approval.
-Establish a Privacy Ombudsman for grievance redressal.

Strengthen Digital Literacy
-Integrate privacy education into school and college curricula.
-Launch public campaigns for awareness.
-Promote Ethical Tech Development
-Encourage startups to follow ethical AI and privacy-by-design principles.
-Provide incentives for companies adhering to high privacy standards.

Collaborate Globally
-Align domestic laws with international norms.
-Participate actively in international privacy forums.

CONCLUSION

The judiciary's intervention to address the right to privacy in India came at a pivotal moment, especially as the country increasingly adopts digital governance. The growing number of internet users underscores the population's shift toward technology-driven systems. In light of this, the creation of a privacy ombudsman could serve as an effective interim measure to ensure that governmental authorities do not misuse their power, particularly as the legislature works on enacting comprehensive privacy laws.

A comparable mechanism exists in the United Kingdom, where the Investigatory Powers Tribunal—a judicial body—oversees state surveillance and ensures individual privacy rights are upheld. Such institutions are also empowered to supervise the decryption of data, where courts may require law enforcement agencies to provide credible and sufficient evidence justifying such action. This ensures that surveillance or intrusion is warranted and not arbitrary.

Within the European Union, competition law analysis extends beyond traditional pricing metrics. The EU evaluates market practices using a five-fold framework—price, output, quality, consumer choice, and innovation. The rationale is that companies, when allowed unchecked access to user data, might lower service quality or limit choices, which in turn affects consumer welfare. Therefore, antitrust regulations become relevant when such deterioration arises due to monopolistic behavior or corporate mergers.

Several key mergers—Microsoft-Skype, Facebook-WhatsApp, and Microsoft-LinkedIn—have been scrutinized in the EU under this broader lens, focusing on non-price factors such as data usage and user privacy. To further protect personal data, the EU has implemented the General Data Protection Regulation (GDPR), a landmark framework that emphasizes user control, transparency, and data accountability.

India, too, proposed similar measures in its Personal Data Protection Bill, which aimed to establish a Data Protection Authority. This authority would be responsible for guarding individual rights against data misuse and ensuring compliance by digital entities. The draft also included penalties for unauthorized data processing, unlawful data sharing, and the re-identification of anonymized data without explicit user consent. However, the Bill was later withdrawn to incorporate more refined provisions through a future iteration of the legislation.

India is currently navigating a path that balances citizen privacy protections with national security imperatives. By drawing on best practices from international jurisdictions—such as the EU's comprehensive data policies and the UK's oversight models—India can construct a robust data governance ecosystem. Not only would this framework secure digital rights for its citizens, but it would also position India as an attractive regulatory hub for global tech companies, contributing to its larger economic ambition of becoming a $5 trillion economy.

REFERENCES

1. Cadwalladr, C., & Graham-Harrison, E. "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach." *The guardian* 17.1 (2018): 22.

Publisher: SARC Publisher

2. European Union. “General Data Protection Regulation (GDPR).” *Regulation (EU) 2016/679*. (2016).
3. Government of India. “Indian Telegraph Act.” (1885).
4. Government of India. “Information Technology Act.” (2000).
5. Government of India. “Digital Personal Data Protection Act.” (2023).
6. IAMAI. “Internet in India Report.” *Internet and Mobile Association of India*. (2023).
7. Internet Freedom Foundation. “Project Panoptic: India's facial recognition systems.” (2021).
8. Ministry of Electronics and Information Technology. “The Personal Data Protection Bill.” (2019).
9. Narayanan, A., & Shmatikov, V. "Robust de-anonymization of large sparse datasets." *2008 IEEE Symposium on Security and Privacy (sp 2008)*. IEEE, (2008).
10. Organisation for Economic Co-operation and Development. “Consumer data and competition: A policy paper.” (2020).
11. Solove, D. J., & Schwartz, P. M. “Information privacy law (6th ed.).” *Wolters Kluwer*. (2020).
12. Software Freedom Law Centre. “Central Monitoring System.” (2020).
13. Srikrishna Committee Report. “Report of the Committee of Experts on Data Protection.” (2018).
14. Stucke, M. E., & Grunes, A. P. “Big Data and Competition Policy.” *Oxford University Press.* (2016).
15. M.P. Sharma v. Satish Chandra, AIR 1954 SC 300.
16. Kharak Singh v. State of U.P., AIR 1963 SC 1295.
17. Gobind v. State of M.P., AIR 1975 SC 1378.
18. Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
19. UIDAI v. “Central Bureau of Investigation,” W.P. (C) No. 494 of 2012.
20. UNICEF. “Children’s data governance: A child rights-based approach to data.” (2021).
21. Indian Computer Emergency Response Team. “Annual Report.” (2022).

Source of support: Nil; **Conflict of interest:** Nil.

Cite this article as:
kumar, A. “Increasing Threat to the Right to Privacy in Digital Age: An Overview." *Sarcouncil journal of Arts humanities and social sciences* 4.8 (2025): pp 43-49.

Publisher: SARC Publisher