SKU JOURNAL OF LEX VIBRENT
April – June 2024
Vol-1
Issue-2

Privacy Rights and the Collection of Personal Data by Tech Companies: An Indian Perspective

Deepti Seth
Assistant professor, Department of Law
Shree Krishna University, Chhatarpur (M.P.)

ABSTRACT

The rise of digital technology and the pervasive use of personal data by tech companies have significantly impacted privacy rights in India. This research paper explores the complex dynamics between privacy rights and the collection of personal data by tech companies, focusing on the Indian context. Utilizing a qualitative methodology, the study synthesizes existing literature, analyzes relevant case studies, cites judicial decisions, and evaluates regulatory frameworks. The paper highlights the evolving legal landscape in India, marked by the landmark *Justice K.S. Puttaswamy (Retd.) v. Union of India* case, which recognized privacy as a fundamental right under the Indian Constitution. It also examines the Personal Data Protection Bill (PDPB) of 2019 and its implications for tech companies' data collection practices. The discussion addresses the tension between privacy and innovation, the commodification of data, and the role of judicial oversight in shaping privacy norms. The study concludes that while legal frameworks are evolving, further refinement is necessary to balance technological advancement with robust privacy protections.

KEYWORDS

Privacy Rights, Personal Data Collection, Tech Companies, India, Personal Data Protection Bill (PDPB), Data Protection, Legal Framework, Judicial Oversight, Data Commodification.

INTRODUCTION

The digital age has revolutionized the way personal data is collected, stored, and used. In India, as in many parts of the world, tech companies have increasingly come under scrutiny for their role in collecting and processing vast amounts of personal data. The collection of personal data—whether through social media platforms, e-commerce sites, or mobile applications—has led to significant debates surrounding privacy rights. The central issue revolves around how much personal data can be collected, who owns this data, and how it is being used. India, with its rapidly expanding digital economy and large internet user base, faces unique challenges in balancing technological advancement with individual privacy rights.

This paper delves into the intricacies of privacy rights in India, focusing on the role of tech companies in collecting personal data. By analyzing existing literature, examining key case studies such as the landmark judgment in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, and

evaluating the evolving regulatory frameworks, this research aims to explore the current landscape of data privacy in India and the potential pathways for addressing the associated concerns.

Background

Rise of Digital Platforms and Data Collection

The rapid growth of the internet in India has been transformative. Tech companies, especially those operating social media platforms, search engines, and e-commerce sites, rely on user data to optimize their services. The collection of data is not inherently harmful; it is often necessary to improve user experiences, personalize content, and enhance efficiency. However, with increased data collection comes the risk of misuse, leading to violations of privacy rights.

Personal data includes information such as browsing habits, location, financial details, medical history, and even biometric data. The collection of such sensitive information by tech companies—often without explicit consent—has raised concerns about individual autonomy, security, and the potential for exploitation.

Privacy as a Fundamental Right in India

In August 2017, the Supreme Court of India delivered a historic judgment in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, affirming the right to privacy as a fundamental right under Article 21 of the Constitution of India. The judgment marked a watershed moment in Indian jurisprudence, establishing the legal foundation for challenging any form of data collection that infringes on personal privacy.

The *Puttaswamy* judgment was particularly significant in the context of growing digital surveillance and the indiscriminate collection of data by both the government and private entities. The Court's decision has shaped subsequent debates on the role of tech companies and data protection laws in India.

METHODOLOGY

This research employs a qualitative methodology, synthesizing existing literature, analyzing case studies, citing decided cases and their judgments, and evaluating regulatory frameworks. The study involves a comprehensive review of academic articles, legal documents, policy guidelines, and reports from advocacy groups. The aim is to provide a comprehensive analysis of the privacy challenges posed by data collection in the Indian context.

LITERATURE REVIEW

Theories on Privacy and Data Collection

The academic discourse around privacy in the digital age primarily revolves around the balance between technological innovation and individual rights. Scholars such as Daniel Solove and Julie

Cohen argue that privacy is not only about protecting information but also about maintaining individual autonomy in a highly digitized society. Solove's taxonomy of privacy breaches categorizes different forms of privacy violations, from surveillance to information dissemination, which are relevant when discussing the role of tech companies in collecting personal data.

In the Indian context, privacy theories have been closely linked to constitutional law and the evolving nature of fundamental rights. Scholars such as Usha Ramanathan have examined the impact of data collection practices in India, particularly in relation to Aadhaar, the world's largest biometric ID system. The intersection of privacy, state surveillance, and corporate data collection remains a key area of concern in India's legal and academic circles.

Regulatory Frameworks

India's regulatory framework governing data collection has evolved significantly over the past decade. The Information Technology (IT) Act of 2000, amended in 2008, includes provisions under Section 43A and Section 72A related to data protection and privacy. However, these provisions are often considered inadequate given the current scale of data collection by tech companies.

The Personal Data Protection Bill (PDPB) of 2019, which draws inspiration from the European Union's General Data Protection Regulation (GDPR), is India's most significant legislative attempt to address data privacy issues. The PDPB aims to establish a comprehensive framework for the protection of personal data, providing individuals with greater control over their data while also holding tech companies accountable for breaches. However, the Bill has faced criticism for its potential to allow government overreach and insufficient protection against corporate misuse of data.

Case Studies

Case Study 1: *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017)

The *Puttaswamy* case is central to the discourse on privacy rights in India. It originated as a challenge to the Aadhaar scheme, which required individuals to provide biometric data to access government services. Petitioners argued that the mandatory collection of biometric data violated the right to privacy, particularly because Aadhaar data was being shared with private entities for authentication purposes.

In its judgment, the Supreme Court ruled that the right to privacy is a fundamental right under Article 21, which guarantees the right to life and personal liberty. The Court held that any invasion of privacy must satisfy the test of legality, necessity, and proportionality. While the Court upheld the validity of Aadhaar for government services, it imposed strict limitations on its use by private companies, thus setting a precedent for data protection.

Case Study 2: *Aadhaar and Data Privacy*

The Aadhaar system itself represents a complex case of data collection and privacy. With over a billion citizens enrolled, Aadhaar collects biometric information (fingerprints and iris scans) and links them to a unique identification number. Initially implemented to streamline welfare distribution and reduce fraud, Aadhaar has since expanded to be used by banks, telecom companies, and other private entities for verification purposes.

Critics of Aadhaar have raised concerns about data breaches, unauthorized access, and the potential for surveillance. The 2017 *Puttaswamy* ruling curtailed some of these issues by preventing private companies from using Aadhaar for customer verification, but concerns about government surveillance remain. Moreover, the integration of Aadhaar into various aspects of daily life has led to debates about the erosion of privacy.

Case Study 3: Data Collection by Social Media Platforms

Social media platforms such as Facebook, Twitter, and WhatsApp have become primary sources for personal data collection. In India, these platforms have millions of users, many of whom share vast amounts of personal information without fully understanding how their data is being used.

Facebook's role in the Cambridge Analytica scandal, where data from millions of users was harvested without consent for political campaigns, highlighted the dangers of data collection by social media platforms. While this scandal took place primarily in Western countries, its implications were felt in India, where concerns about political manipulation via social media were already rising. India's response to such incidents has been to push for stricter regulations on how tech companies handle user data, but the effectiveness of these measures remains to be seen.

Case Study 4: Google's Data Collection Practices

Google's data collection practices in India have come under scrutiny for their sheer scale. The company collects data from its search engine, mobile applications, and the Android operating system, which is used by the majority of smartphone users in India. Google uses this data for targeted advertising, personalization of services, and to improve its artificial intelligence algorithms.

However, concerns have been raised about the opacity of Google's data practices. Users often do not know what data is being collected or how it is being used. The company's global dominance makes it difficult for Indian regulators to enforce stricter privacy standards. Nevertheless, the introduction of the PDPB could potentially hold companies like Google accountable for data breaches and misuse.

Legal and Regulatory Challenges

The Personal Data Protection Bill, 2019

The PDPB seeks to provide a comprehensive framework for data protection in India. It mandates the creation of a Data Protection Authority (DPA) to oversee compliance with data protection norms. Under the PDPB, individuals have the right to access their data, correct inaccuracies, and even withdraw consent for data collection.

However, the Bill has faced criticism for provisions that allow the government to exempt itself from certain data protection obligations in the interest of national security. This has raised concerns about the potential for mass surveillance under the guise of security. The Bill's reliance on the principle of consent is also problematic, as many users are unaware of the implications of consenting to data collection by tech companies.

The Role of Tech Companies

Tech companies operating in India are subject to both domestic regulations and the laws of their home countries. Companies like Google, Facebook, and Amazon must navigate the complexities of India's evolving data protection framework while also complying with global privacy standards like the GDPR.

One challenge for tech companies is balancing their business interests with privacy obligations. Data is often referred to as the "new oil" because of its immense value in the digital economy. Tech companies rely on data to offer personalized services and targeted advertising, which are major revenue streams. However, this reliance on data has led to significant privacy violations, as evidenced by various scandals involving unauthorized data sharing and breaches.

Judicial Responses to Privacy Violations

The Indian judiciary has played a crucial role in safeguarding privacy rights, particularly in the context of tech companies. The *Puttaswamy* case set a high standard for data protection, but other cases have also addressed the misuse of personal data. For instance, in *Internet Freedom Foundation v. Union of India* (2020), the Delhi High Court emphasized the importance of protecting individual privacy in the face of mass data collection by tech companies.

Courts have also issued injunctions against specific practices that violate privacy, such as the collection of data without explicit consent or the misuse of data for commercial purposes. These judicial interventions have shaped the regulatory environment in India, making it increasingly difficult for tech companies to operate without adhering to privacy standards.

Discussion

The Evolving Concept of Privacy in India

The right to privacy, particularly in the context of the digital age, has emerged as a critical issue in India. Historically, privacy was not explicitly mentioned in the Constitution of India, and its recognition as a fundamental right has been a result of evolving jurisprudence. The landmark judgment in *Justice K.S. Puttaswamy (Retd.) v. Union of India* in 2017 was a pivotal moment, declaring privacy to be intrinsic to Article 21, which guarantees the right to life and personal liberty.

This judicial recognition marked a significant shift, especially as the country witnessed the rapid digitization of its economy and society. As tech companies increasingly began to collect personal data from users, the need for a regulatory framework to protect individual privacy became evident. The *Puttaswamy* ruling underscored the importance of proportionality in privacy violations, stressing that any infringement on this right must be justified by legality, necessity, and a proportional relationship to the aim sought to be achieved. From this ruling, the larger question arose: how do tech companies, often global in their operations but local in their impact, align with the emerging standards of privacy protection in India? This discussion explores the gaps between the legal recognition of privacy rights and the actual practices of data collection by tech companies, which often continue unchecked.

Privacy Versus Innovation: A Delicate Balance

Tech companies operating in India, like their counterparts around the world, depend on vast amounts of user data for targeted advertising, personalization, and the development of artificial intelligence algorithms. Data, often termed the "new oil," is fundamental to these companies' business models. However, the relentless pursuit of data raises significant ethical and legal concerns, particularly when the privacy of users is compromised in favor of corporate profits. One of the key challenges in this regard is that users often remain unaware of the extent of data collected and how it is used. Whether it's through cookies on websites, location tracking via mobile applications, or targeted advertisements on social media platforms, tech companies have access to intimate details of users' lives. The collection of this data—without explicit or informed consent—has been a growing concern.

In India, the situation is complicated by the country's large, digitally literate population, which offers tech companies one of the largest markets for data collection in the world. This provides enormous economic opportunities for companies but also exacerbates the risk of widespread privacy violations. The challenge, therefore, lies in striking a balance between fostering innovation in India's growing digital economy and ensuring that the privacy of individuals is respected.

Data as a Commodity and its Implications for Privacy

One of the most pressing concerns in the discourse surrounding tech companies and privacy rights is the commodification of personal data. In the digital economy, data is currency.

Companies collect and trade user data to optimize advertising, design new products, and influence consumer behavior. This commodification has led to the development of entire industries focused on data analytics, marketing, and AI-based personalization. However, the commodification of personal data fundamentally alters the relationship between users and tech companies.

Instead of merely offering services in exchange for fees, many tech companies now provide "free" services in exchange for data. Platforms like Google, Facebook, and Instagram offer free use of their applications, but the cost is borne in terms of privacy, as user data is collected for personalized advertisements and other forms of monetization. Users often do not fully comprehend this trade-off, especially when terms and conditions are lengthy, complex, and opaque. This creates an environment in which data is commodified without explicit, informed consent, raising important questions about user autonomy and the ethical responsibilities of tech companies.

Legal Frameworks and Their Adequacy

In response to the growing concerns about privacy and data collection, India has attempted to establish a comprehensive legal framework to regulate data protection. The Personal Data Protection Bill (PDPB) of 2019 is the most significant legislative step taken so far. Modeled partly on the European Union's General Data Protection Regulation (GDPR), the PDPB seeks to address the lacunae in India's data protection laws, which have traditionally been governed by the Information Technology (IT) Act, 2000.

The PDPB introduces important concepts such as data localization, data fiduciary responsibilities, and user consent. It also mandates the creation of a Data Protection Authority (DPA) to ensure compliance. By giving individuals more control over their data—such as the right to access, correct, and erase personal information—the PDPB aims to create a regulatory environment that balances privacy rights with the interests of tech companies and the government.

However, the PDPB has not been without its critics. One of the most contentious aspects of the Bill is its provision allowing the government to exempt itself from certain data protection obligations in the interest of national security or public order. This provision has been criticized for potentially enabling state surveillance, raising questions about the effectiveness of the Bill in truly protecting privacy. Moreover, the Bill's emphasis on consent has been seen as insufficient, particularly in a country where digital literacy levels are not uniform. Many users may not fully understand what they are consenting to when they agree to the collection of their data by tech companies.

The legal framework governing data privacy in India is still evolving, and it remains to be seen how effectively the PDPB will address the myriad challenges posed by tech companies' data collection practices. In the meantime, the judiciary has played a crucial role in filling the

gaps, as evidenced by judgments like *Puttaswamy*, which impose important limitations on the use of personal data by both the government and private companies.

The Role of Tech Companies in Shaping Privacy Norms

Tech companies are not merely passive actors responding to regulatory changes—they play an active role in shaping privacy norms through their practices and policies. For instance, in the aftermath of the Cambridge Analytica scandal, Facebook implemented significant changes to its data privacy policies. Similarly, Google has faced global scrutiny over its data collection practices, prompting the company to introduce new privacy controls for users.

In India, however, the adoption of strong privacy norms by tech companies has been slower. Although companies like Google and Facebook have introduced privacy policies and controls, there is often a significant gap between the stated policies and the actual practices of data collection and sharing. This has led to growing concerns about the effectiveness of self-regulation by tech companies.

Furthermore, tech companies often engage in data-sharing agreements with third-party advertisers, raising questions about the extent to which user data is being monetized. In many cases, users are unaware that their data is being sold to third-party entities, which use the information for targeted advertisements and other commercial purposes. This lack of transparency further complicates the relationship between users, tech companies, and privacy rights.

The Role of Judicial Oversight

The Indian judiciary has played a crucial role in addressing the legal and ethical challenges posed by the collection of personal data. The *Puttaswamy* case is perhaps the most important example of this, but other cases have also highlighted the need for greater judicial oversight of data collection practices.

One significant issue is the extent to which tech companies should be held accountable for data breaches and privacy violations. While the PDPB outlines penalties for non-compliance, the judiciary has often been called upon to adjudicate specific cases of privacy violations. Courts in India have taken a firm stance on the need to protect individual privacy, but the rapid pace of technological change means that the legal system is often playing catch-up.

For instance, cases involving social media platforms and their role in spreading misinformation or enabling unauthorized data collection have frequently landed in court. The Indian judiciary's response to these cases has varied, but there is a growing recognition of the need for a more robust legal framework to address the challenges posed by tech companies.

The Way Forward: Striking a Balance

As India moves towards becoming a digital economy, the protection of privacy rights in the face of widespread data collection by tech companies will remain a central issue. The challenge lies in striking a balance between encouraging technological innovation and safeguarding the fundamental rights of individuals.

The Personal Data Protection Bill, while a step in the right direction, requires further refinement to address concerns about government overreach and corporate misuse of data. In addition to legislative reforms, there is also a need for greater public awareness about privacy rights and the risks associated with data sharing. Digital literacy initiatives can play an important role in empowering individuals to make informed decisions about their data.

Finally, tech companies themselves must take greater responsibility for ensuring that their data collection practices respect user privacy. Self-regulation, while not a substitute for legal oversight, can help establish industry norms that prioritize privacy. By fostering a culture of transparency and accountability, tech companies can contribute to creating a digital ecosystem that respects both innovation and individual rights.

CONCLUSION

The intersection of privacy rights and data collection by tech companies presents a complex challenge for India. While the digital age has brought about immense benefits, it has also raised serious questions about the protection of personal information. The recognition of privacy as a fundamental right in *Puttaswamy* and the introduction of the Personal Data Protection Bill represent important steps towards addressing these concerns. However, further work is needed to ensure that India's regulatory framework is robust enough to protect individuals from privacy violations by both the state and private entities. As tech companies continue to play an influential role in shaping the digital landscape, the need for strong privacy protections has never been greater.

WORKS CITED

- Bhatia, Gautam. *The Transformative Constitution: A Radical Biography in Nine Acts*. HarperCollins India, 2019.
- Ramanathan, Usha. "Aadhaar and the Right to Privacy." *Seminar*, vol. 705, 2018, pp. 14-19.
- Solove, Daniel J. *Understanding Privacy*. Harvard University Press, 2008.
- "The Personal Data Protection Bill, 2019." Ministry of Electronics and Information Technology, Government of India, 2019.
- *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.