International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Achieving Transparency in the Data Broker Industry: A Legal Perspective on Regaining Control under the DPDP Act, 2023

Anand Geo[1], Sangeeth Soby[2]

Abstract: ***The data broker industry, while integral to the digital economy, operates largely in obscurity, posing significant challenges to individual privacy. This research article examines the transparency issues inherent in data broker practices, focusing on how individuals, known as data principals, can regain control over their personal data under the Digital Personal Data Protection Act (DPDPA) 2023. The paper explores the deficiencies of current regulations, the risks posed by the opaque and shady nature of data brokers, and suggests legal remedies. Drawing comparisons with the General Data Protection Regulation (GDPR) in the European Union, the paper proposes ways to strengthen India's regulatory framework and protect data principals from exploitation.***

Keywords: Data brokers, Privacy, Digital Personal Data Protection Act, Regulation, Transparency

1. Introduction

The rise of data brokerage has reshaped the digital economy, enabling companies to profile consumers, predict behaviours, and tailor services based on vast quantities of personal data. However, the transparency of this process remains highly questionable. Data brokers acquire personal information without the direct knowledge or consent of the individuals involved, often bypassing traditional mechanisms of accountability and privacy. These entities collect data from multiple sources, such as public records, social media, and other digital footprints. Then sell it to third parties for purposes that may range from targeted advertising to credit risk assessments. This lack of transparency places data principals at risk, these practices bring in legal and ethical concerns.

India's recent enactment of the Digital Personal Data Protection Act (DPDPA) in 2023 marks a significant step towards protecting personal data. However, the act falls short in addressing the specific challenges posed by data brokers, leaving individuals vulnerable to unauthorized and opaque data practices. This paper seeks to analyse these gaps, examine how the DPDPA can be strengthened to bring more transparency to the data broker industry, and provide solutions that empower data principals to regain control over their personal data.

The Dark Side of Data Brokers

Data brokers operate in a complex ecosystem that trades on the value of personal data. The primary issue with this industry is the lack of transparency in how data is collected, processed, and sold. Unlike traditional data fiduciaries; that interact directly with data subjects, data brokers often obtain personal data indirectly from third - party sources, making it difficult for individuals to track how their data is being used.

The most serious concern in this scenario is the lack of consent. Data brokers rarely obtain direct consent from data principals. Instead, they aggregate data from multiple sources where consent may have been granted under terms far remote from the ultimate use of the data. This disconnects in consent allows data brokers to operate in a legal grey area, exploiting personal data without the data principal's explicit knowledge or approval[1].

Another risk posed by the data broker industry is identity theft and profiling. By collecting vast amounts of personal information, data brokers create detailed profiles that may include financial details, health information, and behavioural patterns. Once aggregated, this data can be sold to companies, advertisers, or even governmental agencies, often without the knowledge or consent of the individual involved. The potential for misuse is significant, ranging from discriminatory profiling to targeted marketing that manipulates consumer behaviour[2].

In this context, the lack of transparency exacerbates the privacy risks, leaving data principals with limited recourse to regain control over their personal data. This calls for a legal framework that imposes stricter transparency obligations and accountability mechanisms on data brokers. The DPDP Act 2023, only talks about the digital personal data, but personal data is also available in the form of non - digital data, which is later converted into digital forms, and sold to third - parties.

The Digital Personal Data Protection Act (DPDPA), 2023

The DPDPA 2023 represents India's attempt to regulate personal data processing and strengthen the privacy rights of individuals. The act outlines several rights for data principals, including the right to access, correct, and erase personal data. It also imposes obligations on data fiduciaries to ensure that data is processed lawfully, securely, and transparently. However, while the act provides a robust framework for data protection, it falls short in addressing the specific challenges posed by the data broker industry. The act highlights the importance of collecting consent of the data principal, but what can be done when the data brokers aren't the ones

[1] Solove, D.J. (2013). Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, 1880.

[2] Schwartz, P.M., & Solove, D.J. (2011). The PII Problem: Privacy and a New Concept of Personally Identifiable Information. *New York University Law Review*, 1813.

collecting at the collection point, they collect the data at a later stage. This is why it is difficult for to track these brokers and bring them under regulation. They mainly deal in the unregulated black market of data sellers and buyers. One of the key features of the DPDPA is the consent requirement. The act mandates that data principals provide explicit and informed consent before their data is processed. However, the application of this provision to data brokers remains unclear. Data brokers often acquire data indirectly, through third - party transactions where the original consent may not extend to subsequent uses. This creates a legal loophole, allowing data brokers to evade the robust consent mechanisms intended to protect data principals[3].

The DPDPA also provides for data principal rights, such as the right to request access to personal data and the right to request its deletion. While these rights are crucial, their enforcement against data brokers presents a challenge. Many individuals are unaware that data brokers hold their data, and even when they do, tracking down how the data was obtained and where it has been shared can be an impossible task. Unlike the GDPR, which mandates stringent consent tracking and transparency in third - party data sharing, the DPDPA lacks similar enforcement mechanisms that could hold data brokers accountable[4].

Additionally, the act's provisions on cross - border data transfers offer some protection, but they are not sufficiently comprehensive to regulate data brokers who frequently transfer personal data across jurisdictions. The absence of stringent regulations on cross - border data sharing increases the risks of data misuse in international contexts, especially when data is transferred to countries with weaker data protection laws[5].

Regaining Control Over Personal Data

To regain control over their personal data, data principals must be empowered with more than just theoretical rights; they need practical tools that are enforceable. The GDPR provides a useful model in this regard, particularly through its data subject rights and data minimization principles. The DPDPA should incorporate similar mechanisms to ensure that data brokers are held accountable for how they collect and use personal data.

Strengthening consent requirements is the first step towards achieving this goal. While the DPDPA mandates explicit consent, data brokers often operate outside the direct consent framework. The DPDPA should be amended to impose stricter obligations on data brokers, ensuring that they secure verifiable, granular consent before processing or selling personal data. This would involve creating an unbroken chain of consent that follows the data throughout its lifecycle, from the initial collection to any subsequent transactions[6].

Moreover, enforcing data principal rights requires that data brokers be held to the same standards as other data fiduciaries. The DPDPA must impose transparency obligations on brokers, compelling them to inform individuals when their data is collected, sold, or transferred. A right to be informed, similar to that found in the GDPR, would ensure that data principals are notified every time their data changes hands. Furthermore, the DPDPA should enhance its right to erasure provisions, allowing individuals to request the deletion of their data from data brokers' databases in a simple, accessible manner[7].

Another critical area that requires reform is cross - border data protection. The DPDPA's provisions for cross - border data transfers should be expanded to impose greater accountability on data brokers. Following the GDPR's model, the act should require that any entity receiving personal data from India adheres to equivalent data protection standards, ensuring that Indian citizens' data is protected no matter where it is processed[8].

Legal and Regulatory Solutions

To address the opacity in the data broker industry, a combination of legal reforms and regulatory oversight is necessary. Even though the data protection board of India will be formed under the Act, the government must establish a dedicated regulatory body tasked with overseeing the activities of data brokers, this can be a separate body or a sub body created under the Data Protection Board of India (DPBI). This body would be responsible for ensuring compliance with transparency and consent requirements, conducting audits, and imposing penalties for violations. Such a regulatory body could also serve as a point of contact for data principals, helping them exercise their rights and resolve disputes with data brokers[9]. The DPBI must being out the data brokers that are in the shadows, regulation is only achievable post identifying the shadow actors, and bringing them out in the light will make them comply to the rules.

Additionally, the creation of data principal portals would enhance transparency by allowing individuals to manage their data directly. These portals, mandated under the GDPR, allow data principals to access, correct, or delete their data through a centralized system. Implementing similar portals in India would empower individuals to regain control over their data and increase accountability for data brokers[10].

Public awareness campaigns are also critical. There must be efforts to educate individuals about their rights and the risks posed by data brokers. Empowering data principals through

[3] Srikrishna Committee (2018). *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*.
[4] Regulation (EU) 2016/679, General Data Protection Regulation (GDPR).
[5] Narayanan, A. (2019). The Future of Cross-Border Data Flows: Data Localization v. Free Flow of Data. *Journal of International Economic Law*, 22(2), 374.
[6] Tene, O., & Polonetsky, J. (2012). Privacy in the Age of Big Data: A Time for Big Decisions. *Stanford Law Review Online*, 64(63).
[7] Pasquale, F. (2015). *The Black Box Society: The Secret Algorithms That Control Money and Information*. Harvard University Press.
[8] Regulation (EU) 2016/679, General Data Protection Regulation (GDPR).
[9] Srikrishna Committee (2018). *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*.
[10] Tene, O., & Polonetsky, J. (2012). Privacy in the Age of Big Data: A Time for Big Decisions. *Stanford Law Review Online*, 64(63).

knowledge will ensure that they take proactive steps to protect their data and hold data brokers accountable[11].

2. Conclusion

The data broker industry presents significant challenges to privacy and data protection, particularly in the context of consent, transparency, and control over personal data. While the DPDPA 2023 provides a solid foundation for data protection in India, it requires further reforms to address the unique challenges posed by data brokers. Strengthening consent mechanisms, enhancing transparency obligations, and enforcing data principal rights are essential to ensuring that individuals can regain control over their personal data. By drawing on international best practices, such as those found in the GDPR, India can create a more robust regulatory framework that holds data brokers accountable and protects the privacy of data principals.

[11] Schwartz, P.M., & Solove, D.J. (2011). The PII Problem: Privacy and a New Concept of Personally Identifiable Information. *New York University Law Review*, 1813.