
ILLUSION OF CONSENT IN DIGITAL LENDING: RETHINKING DATA GOVERNANCE UNDER INDIA'S DPDP ACT

Renuka Kumari, Research Scholar, Symbiosis Law School, Noida Campus, Symbiosis International (Deemed University), Pune, Maharashtra, India

Dr. Aayushi Goel, Assistant Professor of Law, Symbiosis Law School, Noida

ABSTRACT

The rapid expansion of fintech in India has helped to increase access to formal financial credit for millions of borrowers who had been denied such access. However, this access rests on an increasingly uncomfortable foundation; the continuous extraction of personal data as a condition of financial participation. This commentary examines the notice and consent framework of the Digital Personal Data Protection (DPDP) Act 2023 as it operates within digital lending ecosystem. It argues that although consent is made obligatory under section 6 of the Act, it is more of a formalistic requirement than a genuine expression of autonomy because of the position of dependence of borrowers and the dominance of lenders. The bundled permissions embedded in fintech interfaces normalize extensive data extraction and thus produces the 'privacy for credit' trade-off of power in the credit ecosystem. By examining the data credit nexus, the current commentary shows financial inclusion is increasingly mediated through behavioral visibility. It argues that there is a need to move beyond the regime of consent and towards institutional responsibility as the organizing principle of fintech governance.

Keywords: Digital Personal Data Protection Act (DPDP), Digital Lending, Financial Inclusion, Data-Credit Nexus, Consent Architecture, Behavioral Data, Platform Dominance, Fintech Governance, Privacy for Credit.

The Illusion of Consent in Data Driven Finance

The rapid growth of fintech in India is mostly described as a narrative of technological inclusion. The proliferation of Unified Payments Interface (UPI) platforms, app based lending and embedded credit products have drastically lowered the transaction costs of borrowing. The small ticket loans are cleared out within minutes, first time borrowers are brought into formal credit systems and alternative data is advanced as a remedy to the 'thin file' problem that has historically locked out informal workers in institutional finance. This change is closely connected to the larger digital public infrastructure (DPI) of India which incorporates payment systems, digital identity, and data sharing systems to increase financial access. The credit architecture has also changed fundamentally over that of traditional lending that was dependent upon collateral, verified income, or personal relationships to evaluate borrowers. Digital lending focuses on behavior as a way of measuring creditworthiness rather than using any of the traditional methods. Therefore, credit decisions increasingly depends on digital visibility rather than collateral. This can be described as a 'privacy for credit' trade-off which represents the exchange of financial access for continuous behavior visibility. Regulatory developments have started to reflect the challenges posed by this transformation.

The Reserve Bank of India (RBI) issued the Digital Lending Guidelines in 2022 due to numerous customer complaints about non-transparent lending practices, excessive data acquisition and coercive recovery techniques associated with many digital lending applications. This regulatory action highlights that the traditional self regulation existing in fintech markets can no longer adequately serve the needs of consumers as these fintech industries continue to be disrupted with rapid growth. Furthermore, the concentration of a limited number of lending platforms in UPI transaction activities continues to solidify the role of app based intermediaries within everyday financial transactions. The workings of digital lending platforms take the form of standardized, non-negotiable interfaces which look like 'contracts of adhesion', with access to credit being conditional on the acceptance of bundled permissions. This shows that there is a deeper difference between voluntariness as a form and voluntariness, evidenced by the clicking 'accept', is mediated by economic necessity, choice limitation, and the dominance of digital financial platforms. Here, consent plays a dual role by providing access to the credit and also enabling the normalization of extensive data extraction. The real issue, then, is not whether consent exists, but whether it can ever be effective as a form of voluntariness within an asymmetric digital credit market.

The Consent Architecture of DPDP Act and Its Structural Constraints

The Digital Personal Data Protection Act, 2023 (DPDP Act) is the key legal instrument in India's digital economy which regulates the processing of personal data.¹ The law takes a consent based approach whereby individuals would be called 'data principals' and organizations using personal data as 'data fiduciaries'.² Section 6 of the Act provides that the personal data can be processed only by a free, specific, informed, unconditional, and unambiguous consent, but it must be announced in advance in accordance with Section 5 specifying the nature and purpose of collecting data.³ This model employs the principle of informational self determination whereby the individual is put at the center of data control, however, in reality its functioning in the digital lending ecosystem demonstrates a number of structural constraints.⁴ The notice requirement, required to be given in English or in any of the languages mentioned in the Eighth Schedule of the Constitution, can lead to very lengthy and technically complicated disclosures. Privacy documents tied to lending applications often go beyond a length of several pages and include very technical explanations of how the data is processed and such notices hardly amount to meaningful understanding among borrowers in informal or gig economies who depend on app based credit. Thus, consent can be formally acquired but the substantive knowledge still remains minimal. The other conflict is based on the Act's provision on 'certain legitimate uses'.⁵ The law allows processing of the data which individuals have knowingly given their personal information for a certain purpose, and they have not refused the use of their data otherwise. This provision creates a regulatory grey area in the fintech environment. Platforms often argue that by applying for credit or using financial apps, users have willingly made themselves available to digital records like history of transactions, device IDs or metadata of their behavior. Contemporary machine learning models ingest precisely such behavioral and transactional signals including digital banking activity and device metadata enabling profiling that extends well beyond conventional financial measurements.⁶

¹ Digital Personal Data Protection Act, 2023, No. 22 of 2023, Gazette of India, Extraordinary, Part II, sec. 1.

² Id. § 2.

³ Id. §§ 5–6.

⁴ Ajay Kumar Bisht & Neeruganti Shanmuka Sreenivasulu, Information Privacy Rights in India: A Study of the Digital Personal Data Protection Act, 2023, in DATA PRIVACY – TECHNIQUES, APPLICATIONS, AND STANDARDS (2024).

⁵ Digital Personal Data Protection Act, 2023, § 7(a).

⁶ Sayyed Khawar Abbas, Lending by Algorithm: Fair or Flawed? An Information Theoretic View of Credit Decision Pipelines, 6 SN COMPUTER SCI. (2025).

The consent framework is also complicated by institutional arrangements in India's digital financial infrastructure. The Account Aggregator (AA) ecosystem is governed by Reserve Bank of India's *Master Direction on the NBFC Account Aggregator* and is used to share financial information on a consent basis among the regulated entities.⁷ Although this is meant to increase the consumer control on financial information, it is also creating a stratified regulatory framework with the RBI monitoring the flow of financial information and the Data Protection Board dealing with privacy breaches.⁸ The policy focus on increasing the digital credit flows may weaken the efficacy of withdrawal rights and strengthen the reliance of the borrowers on the system of data sharing. Significant Data Fiduciaries are also introduced by the Act, requiring large platforms who are dealing with huge volumes of personal data to take further action such as data protection impact assessments and appointing data protection officers. Nevertheless, these requirements have little effect on structural incentives that foster large scale data extraction rather they enhance internal governance and documentation behaviors. The DPDP Act on the one side strengthens the procedural consent, but on the other it does not change much regarding the wider asymmetries of platform concentration, behavioral profiling, and economic dependency, which shape the meaning of consent in digital credit markets.

The Political Economy of Fintech Data Governance

To fully grasp the constraints on consent concerning digital lending, it's crucial to place data use of fintech companies among the broader political economy of credit allocation. The development of data based credit scoring, instead of collateral based lending, is not only a technological change, but also an action that reorganized the authority of credit allocation. Traditionally, the creditworthiness was determined using assets, reported income or relationship knowledge between borrowers and lenders. Under platform based finance, however, reputational capital that is based on the digital traces is replacing physical collateral more and more.⁹ The history of transactions, device identifiers, location signals, consumption behavior and trends of digital interaction are pooled together to create probabilistic risk scores. This nexus is strongly connected to the digital financial infrastructure institutional setup of

⁷ Reserve Bank of India, *Master Direction – Non-Banking Financial Company – Account Aggregator* (Reserve Bank) Directions, 2016.

⁸ Aashi Dixit, *Data Protection in India After the Digital Personal Data Protection Act, 2023: A Critical Evaluation of Privacy and State Power*, 6 INDIAN J. LEGAL REV. 116 (2026).

⁹ Aashi Dixit, *Data Protection in India After the Digital Personal Data Protection Act, 2023: A Critical Evaluation of Privacy and State Power*, 6 INDIAN J. LEGAL REV. 116 (2026).

India. Unified Payments Interface (UPI) which is run by the National Payments Corporation of India (NPCI) has turned out to be the core of digital payments in the country and even though UPI is intended to be an interoperable public infrastructure, the retail market is highly concentrated. By March 2026, the volume of UPI transactions through PhonePe and Google Pay accounts for about 45.5% and 34.6% of the total volume digital payment transactions. Upon acknowledging the dangers of this concentration, NPCI proposed a limit of 30 percent on market share of third party application providers.¹⁰ Compliance dates have, however, been pushed back several times, most recently to 31 December 2026, as a practical response to the challenge of restructuring an already large payments environment dominated by a small number of large platforms. Such recurring extensions are a depiction of how the regulatory frameworks tend to be more reliant on the prevailing intermediaries to sustain digital financial infrastructure.

The amount of data stored in such sites creates strong network effects, the greater the number of users who conduct transactions using a given application, the deeper the behavioral data it has. Larger volumes enable the platform to create more sophisticated predictors and, consequently, get more users, traders, and finance providers. Information is thus a source of credit score inputs and a competitive edge that enforces platform domination. The issues of these so called 'data moats' have dictated regulatory reviews in India. Competition Commission of India (CCI) did an investigation into digital markets which revealed the presence of the gatekeeper function by the dominant platforms. The proposed Digital Competition Bill (2024) introduced the category of Systemically Significant Digital Enterprises (SSDEs) and proposed to limit the practices of using non-public business user data to strengthen market power and impair smaller competitors.¹¹ The predictive algorithms enable identification of borrower behavioral traits and consumption patterns that the borrower might not even be aware of. This 'algorithmic gaze' enables lenders to segment the market and price credit in a sophisticated manner. Data analytics are increasingly empowering lenders to predict borrower behavior and tailor credit terms accordingly. The Reserve Bank of India's 'Framework for Responsible, Explainable, and Ethical AI in the Financial sector' acknowledges the dangers associated with non-transparent algorithmic systems and highlights

¹⁰ National Payments Corporation of India, Standard Operating Procedure (SOP) for Monitoring the 30% Cap on UPI Transactions (2020).

¹¹ Ministry of Corporate Affairs, Report of the Committee on Digital Competition Law (2024).

principles such as fairness, transparency, and accountability.¹² However, this framework primarily addresses these issues from the perspective of institutional governance and risk management offering limited protection for borrowers. This framework does not provide any borrower rights like right to explanations or contestations. The DPDP Act deals with the legality of the data being collected, but there is little room for the interpretation of data being collected for the proprietary credit scoring systems. In such a situation, the concept of consent works more like a tool through which governance is effectively delegated to the private sector. Thus, the political economy of fintech data governance presents a paradox that the digital infrastructure that seeks to advance financial inclusion ends up promoting surveillance capitalism and reinforcing the power of the existing intermediaries.

Beyond Procedural Consent: Toward Structural Accountability

While the DPDP Act provides procedural legitimacy in the form of consent, the more fundamental issue of the governance of digital lending requires the resolution of the issue of the structural imbalance in the Indian fintech market. The major problem with the present system is the dependence of the system on consent in the presence of high concentrations of fintech platforms, the absence of transparency in the decision making of these platforms, and the dependence of the borrowers. Thus, the burden of protecting the personal data of the borrowers is placed on the borrowers themselves, who have limited bargaining power and alternatives.¹³ Enhancing governance would involve changing the concept of individualized consent to institutional responsibility and one of the initial measures is to increase the fiduciary duties of the platforms used to process financial information. Although the DPDP Act refers to such entities as data fiduciaries, the practical meaning of this term is rather small. Digital lending marketplaces control access to credit, the evaluation of risk and the fee framework, which puts them in a position of great economic control. Their data practices should be more effectively regulated because of this functional role. Information gathering that is scarcely related to creditworthiness including rich behavioral metadata or even machine level analytics cannot be justified on the basis of user approval only.¹³ Second, there should be more transparency in algorithmic decision making. The most significant impacts of data processing

¹² Reserve Bank of India, Framework for Responsible, Explainable, and Ethical AI in the Financial Sector (2025). ¹³ Aashi Dixit, Data Protection in India After the Digital Personal Data Protection Act, 2023: A Critical Evaluation of Privacy and State Power, 6 INDIAN J. LEGAL REV. 116 (2026).

¹³ Sayyed Khawar Abbas, Lending by Algorithm: Fair or Flawed? An Information Theoretic View of Credit Decision Pipelines, 6 SN COMPUTER SCI. (2025).

are not in the collection stage but in the credit scoring and pricing stage. Framework for Responsible, Explainable, Ethical AI (2025) recognizes the risks posed by opaque algorithmic systems rather than the rights of borrowers. Digital lending systems need to create accountability through independent algorithmic audits and better explanations of their automated decision making processes. Organizations must address data governance issues together with their market power assessment processes. The Competition Commission of India currently investigates data concentration together with network platforms based on ongoing discussions about the Digital Competition Bill. Privacy protection and competition policy need better alignment to solve these problems. Organizations should view consent as a necessary element of institutional obligations. Digital credit markets with knowledge gaps about loan information and borrower dependence require more than the 'I agree' button for effective borrower protection.¹⁴

Conclusion: Reconsidering Consent in Data Driven Credit.

The growth of fintech in India has significantly increased access to formal credit especially for borrowers who were previously barred from institutional finance. However, this integration is becoming more and more dependent on the ongoing handover of behavioral data. Financial inclusion starts to resemble a system where the cost of participation is continuous algorithmic monitoring when data transparency is a condition of credit access and consent cannot be meaningfully denied. Although DPDP Act establishes a crucial procedural framework, consent alone is sufficient to address the underlying causes of platform dominance and borrower dependence. As a result, the difficulty in regulating digital lies in institutional structure rather than simply compliance. The crucial question is whether India's increasing investment in digital public infrastructure will be regulated in the public interest or will continue to serve as a data foundation of highly concentrated private platforms. This tension can only be solved by going beyond procedural consent and toward more robust institutional accountability forms, as determined by current regulatory decisions.

¹⁴ Abbas, *supra* note 6.