IT for Change

Policy Brief

Data Empowerment and Protection Architecture:

Side-Stepping Empowerment for Convenience?

Tanay Mahindru and Anushka Mittal

December 2021

This paper is part of IT for Change's research series on Intelligent Infrastructures, which interrogates essential digital infrastructures that underpin the economy, society, and governance, shedding light on the need to democratically control these building blocks of tomorrow. This project is supported by International Development Research Centre (IDRC) Canada and the Fair, Green and Global Alliance (FGG).

December 2021

Authors

Tanay Mahindru and Anushka Mittal

Conceptual and editorial guidance

Nandini Chami

Review

Anita Gurumurthy and Amay Korjan

Copy editing

Sneha Bhagwat

Design

Sreemoyee Mukherjee

Data Empowerment and Protection Architecture:

Side-Stepping Empowerment for Convenience?

December 2021

Table of Contents

Data Empowerment and Protection Architecture:

Side-Stepping Empowerment for Convenience?

Driven by increased internet access and demand for retail loans, it is projected that the business value of digital lending in India will exceed USD 1 trillion by 2023. One of the factors at the heart of this dynamic expansion is the crucial value of the data generated within the digital medium. A large proportion of Indian citizens did not previously have access to formal credit due to their lack of credit histories and the absence of adequate means to assess their capacity to service debt. Now, new business models are emerging that increasingly capitalize on 'digital exhaust' to inform lending decisions. In other words, businesses are looking to analyze data – both held by the banks of potential borrowers, and generated as a by-product of a borrower's digital transactions – to predict repayment behavior, evaluate credit-worthiness, and consequently, bring new populations into the ambit of formalized financial services.

This model is not new: Kenya's M-Shwari has used 'alternate data sources' such as mobile phone recharge transactions to serve as the basis for loans since 2012. In fact, lenders have traditionally scrutinized the financial history of prospective borrowers on digital platforms, but often through ad hoc arrangements involving the sharing of login information and 'screen scraping' practices. What is new is the institutionalization of such an approach. The 'Open Banking' movement aims to streamline this process, by enabling 'enhanced market capabilities' through 'collaborative banking models which share consumer data through Application Programming Interfaces (APIs)'. By creating standards for the sharing of information such as the 'Payments Service Directives' (PSD2) in the EU and the 'Open Banking Standard' in the UK, governments are moving to establish the legal and technical infrastructures required to better facilitate information sharing between financial institutions. With an emphasis on citizen consent, the envisioned ideal is that these standards will lead to more secure forms of data sharing. This will, in turn, catalyze 'innovative' startup-driven applications in the fintech ecosystem, thereby enabling greater access to a range of financial services, including money management, insurance, and lending.

Recently, India has proposed to implement a similar model to facilitate increased consent-centric data sharing across sectors such as health, telecommunications, and finance through the Data Empowerment and Protection Architecture (DEPA).

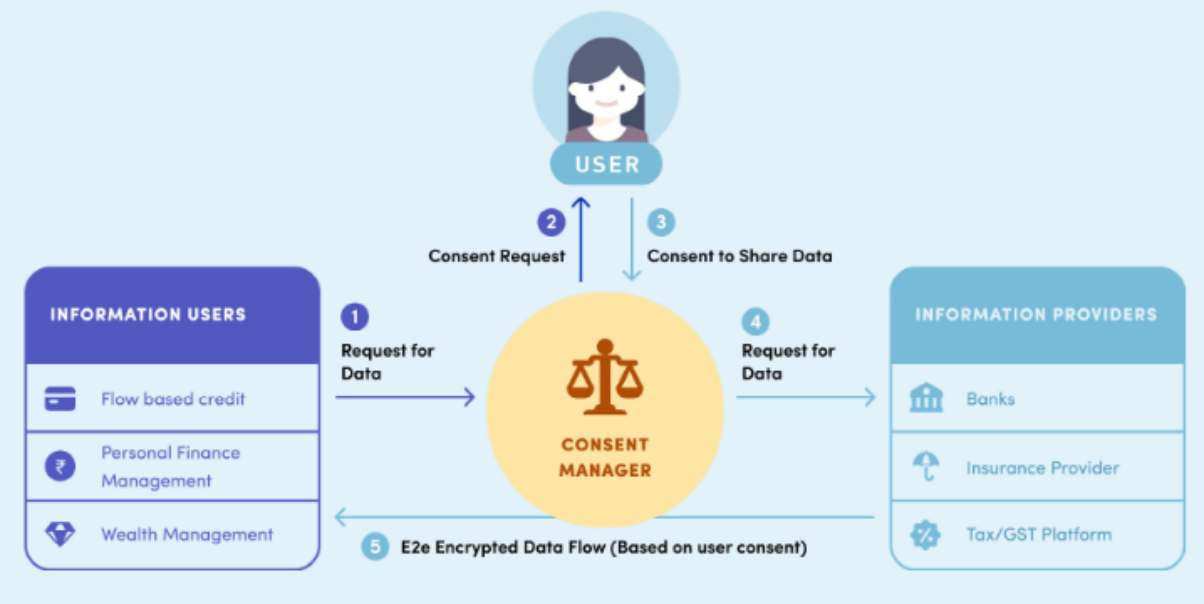
The project's first leg targets the finance sector, where DEPA has been implemented through the Account Aggregator (AA) framework with an explicit mandate to enhance financial inclusion through credit access.

On the face of things, it is certainly true that significant segments of India's population are excluded from networks of formal credit and the combination of digital technology, dynamic start-ups, and a strong public infrastructure have the potential to significantly alleviate this problem. With an initiative such as DEPA, the finer details of its implementation will determine whether it serves as a genuine public good, or it is poised to extend a form of inclusion that would expose some of the country's most vulnerable and marginalized populations to the volatile and dangerous pressures of the predatory, accumulative process driving financial capitalism today. What is the more likely outcome, given the information available? This essay attempts to engage with this question through a careful and critical analysis of DEPA's proposed framework, as well as the proposed regulatory mechanisms envisioned to oversee it.

The Data and Empowerment Protection Architecture: An Overview

Similar to the Open Banking frameworks deployed in Europe, DEPA envisions API standards being available as public digital infrastructure to facilitate the sharing of transactional information and enable services such as access to credit based on this information instead of traditional collateral (a practice which has sometimes been referred to as 'flow-based credit'). Citizens are required to consent to this information sharing, and their consent is framed in a manner that is 'granular, revocable, auditable, and secure'. Non-banking Finance Companies (NBFCs) and affiliated fintech start-ups can then use these APIs to deliver new, more customized lending products to citizens.

How is this to be facilitated? DEPA proposes the creation of a new business entity called 'Consent Managers' (in the finance ecosystem, they will be known as 'Account Aggregators') which will be licensed by the Central Bank of India to help manage user consent and facilitate data sharing. Consent Managers will ensure that user consent is gathered as per the established principles, and 'empower' and 'protect' citizens as they access services that require an element of data sharing. The framework proposes the regulation of Consent Managers and AAs through Self-Regulatory Organizations (SROs), with an explicit role imagined for 'Sahamati', a collective of AAs which is envisioned to 'provide procedural and best practice guidelines for all participating institutions, support organisations to adopt and go live, and continue to foster innovation in protecting data rights.' Eventually, the plan is that relevant data from other DEPA sectors (telecom, education, or jobs) will be routed through these Consent Managers/AAs, forming 'alternate data sources' to inform financial decisions.



A diagrammatic representation of DEPA (Source: DEPA Discussion Paper).

The graphic above illustrates DEPA in a clear and synoptic manner. The 'Consent Manager' bodies, once they secure permission from users, will collate their information from across various financial institutions and serve as a repository of data that can be drawn on by third-parties looking to offer novel financial services to India's citizens. The key value-addition envisioned with this set-up is that it substitutes cumbersome legacy documentation requirements for accessing financial services with easy-to-access and quick mechanisms for personal financial data sharing, underpinned by clear safeguards on personal data of users.

'Datafication' of Lending and Challenges of Meaningful Consent

Assurances towards creating widespread ease of access, and a just, secure, and consent-centric handling of user data is key to DEPA's claims to being a public good. Consequently, it is worth exploring whether the projected framework is capable of delivering on these fronts. Here, from the onset, there are a number of concerning elements to contend with.

To begin with, it is ironic that DEPA looks to digital lending to achieve targets of 'banking the unbanked' and improving access to credit. A dependence on smartphones for access to DEPA-enabled services seems to assume universal access to such devices and fails to acknowledge the persisting digital divide that exists within the country. While aspiring to expand digital lending to new frontiers, DEPA seems to ignore that those who lack access to credit are often precisely those who also lack access to digital interfaces. In fact, recent estimates indicate that more than 400 million people have no

access to the internet, with women and rural communities comprising a large portion of this number. On the other hand, approximately 190 million people in India are estimated to be 'unbanked', which – while constituting a massive 11% of the world's unbanked population – indicates that the portion of the population unable to access the internet exceeds the portion that is excluded from formal banking. Consequently, positioning a technology-centered initiative like DEPA as a means of bridging the credit gap invites critical scrutiny.

The problem with proposing digital finance as a motor for inclusion is further exacerbated by credit lending decisions being predicated on the availability of data. Thus, the implementation of the DEPA or AA framework to increase access to credit or other financial services may organize these frameworks in a way that favors those who are already digitally mature and excludes those that are not. For example, women whose access to either banking or digital services has been restricted will likely be unable to furnish the required banking information or have the means to digitally interact with the system. In fact, by increasing the dependence on limited data to represent marginalized groups, the framework may further perpetuate historical inequities, since lack of data itself may become correlated with inability to repay. As these initiatives push towards the usage of data as the arbiter of 'truth' of individual abilities, it is vital that efforts be made to remain cognizant of on-the-ground realities and have them inform policy development.

Similarly, when one looks at the handling of data – basing the foundation of the DEPA framework on 'consent' may also be inherently challenging. By placing the citizen at the center of the transaction, DEPA seems to assume a high degree of digital literacy in India. However, recent studies have indicated that privacy policies are inscrutable to the majority of Indian students. The spate of recent reports of citizens being taken in by elaborate schemes for predatory lending at illegal interest rates also signal a lack of strong regulations (around non-banking financial companies and platform liability) and a lack of awareness about these matters among the general public. Placing the burden of studying the potential benefits or harms of data sharing on citizens may result in more harm than good, as it exposes them to complex markets without first adequately informing them of their rights. Similar to the Indian Bureau of Energy Efficiency's ratings of electrical appliances, data sharing practices ought to require its regulator to take on the role of guiding individuals to better knowledge and decision-making, rather than leaving it completely to market forces and service providers to shape individual experiences on the basis of their business-oriented motivations.

Breaking Monopolies and Disintermediation through DEPA

Another argument bolstering the rationale for an initiative like DEPA is that enforcing data sharing will counteract monopolies that could develop from the accumulated data silos of entrenched financial institutions. In doing so, it purportedly fosters healthy competition within the financial sector, and a dynamic and equitable economic climate overall. This is certainly a desirable outcome, and one that has served as a central claim in the advocacy of open banking globally. That said, there are several things about the proposed DEPA framework that seem unsuited to achieving this aim, and that may even push the industry towards more dangerous directions. It is important to account for exactly how such developments would restructure the landscape of digital finance in India.

Within the outlined model, AAs are to facilitate the flow of information from Financial Information Providers (FIPs) to Financial Information Users (FIUs), contingent on consumer consent. In doing so, the model further perpetuates a sort of intermediation where there was previously none. This has already been seen in the case of the platformization of transport aggregators, online ticketers, digital property aggregators, etc. (such as Expedia or Airbnb) and in open banking or the larger 'fintech' ecosystems across the world. Though such tasks were previously 'unorganized' (and, thus, free of cost), the current DEPA framework makes provisions for Consent Managers to be able to charge for their services. While the exact business model of the Consent Manager remains unclear, DEPA alludes to exploring various sources of revenue, including charging the consumers. Though these services will likely start off as 'free' to encourage adoption, they will likely move to more concrete business models as they become the predominant means for access to credit.

A case in point is 'FASTag', an electronic toll payment system implemented for Indian highways. Technologically-constructed using a web of linkages between the users' bank accounts and their tag accounts for electronic toll payments, it has also been pushed through by a complex corporate structure, comprising the national highway authority, payments authority, and banks. In its early days, it was incentivized through cashback offers. However, now, it is reasonably predicted that toll concessionaires will inflate the toll charges because each player in the intricate value chain seeks to recoup the costs of service provision.

As with any other digital intermediary and technological solution seen so far, there is an added risk here that transactions through Consent Managers will spiral into a mandatory channel for any service provision. Even though FASTag was introduced in 2014 on an experimental and voluntary basis, it was incrementally enhanced. As of 2021, it has been officially mandated. In fact, any entry of a non-FASTag vehicle (effectively, non-digital payments) in a FASTag lane at a toll plaza is penalized with double the

original amount. Further, it has been rendered compulsory even for availing vehicle insurance or its renewal. This is all the more likely in the case of DEPA-mediated decisions, since FIUs would arguably gather more useful information about users using the digital channel than offline. FIUs may, thus, seek to incentivize this intermediation to request more data from citizens than actually required for providing a specific service, denying services to any individuals that do not comply. A version of this is already seen in the case of 'permissions' required for services mediated through smartphone applications. If users do not give applications the necessary permissions to harvest more data from them, the service is denied outright. As Mr. Srikanth L from Cashless Consumer puts it, "Once the other competing markets are killed out, the AAs will eventually become rent seekers because they will be incentivized and promoted to replace the traditional alternatives. With a comfortable market position, it may assume dominance and exclude based on price, notwithstanding the technological exclusion due to the digital medium".

Similarly, the approach that DEPA takes towards realizing the goal of breaking up data monopolies through increased data sharing is restricted to improving convenience in the sharing of personal information. It focuses on replacing ad hoc data sharing mechanisms such as screen scraping with digitized user journeys. Essentially, the data to be shared is highly tailored and individualized. DEPA does not address issues of disproportionate concentration of behavioral, 'surplus' or 'non-personal' data among a limited number of technology or financial companies, or how citizens can exercise greater control over its usage. Since this information is often of greater value in training algorithms, cross-selling of financial products, and is used for targeted advertising, it is a lost opportunity to truly empower citizens with greater control over their digital footprints and their use. In fact, the current framing of the Consent Managers seems to indicate that they will generate surplus behavioral information themselves, (through their role as intermediaries) and be free to use and trade it unregulated.

Private Sector Participation in the Context of Increased Network Governance

Finally, in being touted as a move to build a strong public infrastructure in the digital domain, DEPA positions itself as part of a vision to harness the power of data and digital platforms in public interest. Allegedly, DEPA aims to establish institutions that are, at least partially, subject to democratic accountability, and which can resist being captured by the logic of the market and corporate power. However, the creation of for-profit entities is at the very heart of this system, and its proposed self-regulation model oversees the activity of these entities. Therefore, one must assess the extent to which the DEPA framework can genuinely keep private interests in check, and the extent of power it concedes to the private sector in governing this domain.

The proposed SRO model for Consent Manager regulation is indicative of a growing affinity to forms of 'network governance' in the digital domain, characterized by a move away from traditional, vertically-integrated, large public sector organizations to more fluid public-private contractual arrangements in discharging core governance functions. In the discourse around public digital goods in India especially, there are concerns that few informally-selected, non-public organizations, founded on the principles of technology optimism, are disproportionately influencing public policy decisions. Research has found that "private technocrats can be encountered in every government office and who, as part of e-government design and implementation teams, confidently wear the face of the Government". It is telling, for example, that DEPA was being articulated by a non-public entity more than a year before there was any mention if it in a Government of India publication. The official government policy document describing DEPA, calls Sahamati out by name as the organization intended to function as the SRO for AAs. Recently, the central monetary authority also released a draft framework for SROs for payment system operators, which highlights benefits of the approach including "expertise", "a higher code of conduct", "communication with market participants", and "enhanced customer experience".

These benefits notwithstanding, a 'soft touch' regulatory approach manifesting itself as an SRO should be avoided, specifically for Consent Managers. As discussed earlier, Consent Manager regulators will need to prioritize guiding customers to informed data sharing practices – particularly since lack of awareness leaves individuals open to instances of exploitation. In addition, the responsibility of managing extremely sensitive citizen information demands that Consent Managers institute robust means of grievance redressal and public consultation – neither of which are typically required of SROs due to their non-public nature. As these entities leave the possibility of being able to charge customers for their services open, a mismatch in incentives highlights another potential challenge in the prioritization of people's rights in regulatory practices. For example, when digital payments were pushed through as part of the policy agenda, banks and payment service providers sought to charge the merchants (and indirectly the consumers) for the digital payment infrastructure that they provided. While the government intervened through the digital payments authority to suspend such charges, it will be interesting to see for how long it will sustain this policy as service providers continue to cite a lack of incentive to provide the requisite infrastructure.

Ultimately, unless a stronger and more independent set of regulatory mechanisms are put in place, DEPA seems unlikely to genuinely function as public infrastructure aiming to empower individuals, and much more so as an enabling environment for a series of private initiatives. Moreover, by reinforcing the trends in network governance, it would be moving in a direction where more and more of the key infrastructure of India's digital economy is vulnerable to dependence on the private sector.

Conclusions and Recommendations

A large proportion of Indians remain 'unbanked', and thus excluded from the ambit of formal financial circuits, and at times from the ambit of formal economic activity. Yet, precisely because of this, they represent a large section of financial flows that remain untapped by the state's tax mechanisms and the profiteering of financial capital. Bringing these masses into the fold is an indispensable part of any project that aims to further the nation's economic development, but if this not done in an adequate manner, they are uniquely vulnerable to being exploited by predatory financial interests.

This context forms the backdrop of our investigation, and having delved into the details of its proposal, we are in better position to address the question with which we started. Does DEPA's projection as a foundational digital finance infrastructure provisioned as a public good have genuine merit? Is it likely to aid the integration of poor and marginalized sections of the population into neoliberal finance markets on exploitative terms?

Based on our analysis, these effects are difficult to imagine. While it is true that the model for digital finance envisaged by DEPA is not yet operational and is liable to being redefined and developed, the set of rules and regulations on which it is currently based are somewhat problematic. As we have tried to show over the course of this paper, the proposed framework focuses on increased datafication, without concomitantly developing basic infrastructure and regulatory systems, or accounting for possible technological exclusion. Given the persisting digital divide, the wide gaps in digital literacy, and the absence of a data protection law, there is little assurance that this push for datafication will significantly boost financial access, or manage to keep propensities for data to be misused by corporations in check.

Moreover, when it comes to dismantling data monopolies, DEPA remains at the level of personal data and completely overlooks the valuable behavioral surplus information and non-personal data also traded as part of the financial data sharing markets. It also does not seem to provide individuals with genuine ownership or control over the ways in which their data is used. To make matters worse, through its Consent Manager entities, it seems to institute a form of financial intermediation that creates perverse incentives for profiteering, and seems vulnerable to generating various kinds of anti-competitive behavior.

Finally, with its proposed 'soft-touch', 'self-regulatory' oversight mechanisms, DEPA refrains from committing to substantive and in-built public accountability. Its model fails to establish the kind of independent regulatory body that can ensure informed decision-making among the citizenry, which ought to be a crucial prerequisite for any initiative of this sort. Rather, by pushing in the direction of

public-private network governance, the proposed framework consolidates long-term dependence on private actors, and their growing influence over the nation's digital finance-ecosystem.

Keeping all of this in mind, DEPA seems to fall short of being able to deliver on the kind of promises that are being made on its behalf. There are many stepping stones between using data to access financial services and real, empowering financial inclusion. Unless considerably restructured in the coming months, or positioned as just one step in a larger road-map to achieving financial self-dependence, it is hard to see DEPA as anything but an attempt to leverage a social gap affecting many, for the economic benefit of a few.

Recommendations

1. **Avoid self-regulation:** The current governance model of Consent Managers envisages a prominent role for self-regulatory organisations (such as Sahamati in the financial sector) for the creation of procedural guidelines and best practices. Given the mixed incentives of Consent Managers, this approach must be avoided in favour of stringent government regulators to ensure the protection of citizen rights while maintaining accountability. While regulators in some sectors, such as the RBI in finance, may have the technical capacity required to enforce norms on the Consent Manager industry, this capacity may be lacking amongst regulators in sectors such as health and agriculture, further highlighting the need for a strong independent regulator.

2. **Establish a clear duty of care:** There is a need to create and enforce regulations that clearly lay out a fiduciary responsibility for entities operating as Consent Managers, to ensure that they act toward the protection of citizen-users they represent. These regulations may extend to the design practices adopted by these entities. For example, the use of 'dark patterns' to nudge users to share data should be strictly prohibited. This mandate must be legally enforced since financial incentives may be at cross-purposes with enacting fiduciary responsibility.

3. **Regulate aggregate or non-personal data:** Data generated during the use of Consent Managers should not be sold to third parties or cross-sold to internal business units of information providers or users for the customization and improvement of services. Currently, the scope of guidelines is restricted to personal data only. However, in recognition of the economic value of non-personal data and potential for large companies to utilize their data monopolies to gain an unfair advantage (as highlighted by the Report by the Committee of Experts on Non-Personal Data Governance Framework, December 2020), regulation must encompass aggregate data within its ambit.

4. **Take steps to prevent monopolization:** Steps must be taken to ensure that the Consent Manager industry is not monopolized by large tech firms across sectors. Clauses to ensure interoperability notwithstanding, upper limits may be placed on market shares of firms in the space, akin to measures that have been instituted for the Unified Payment Interface (UPI). These will help ensure that ostensibly open public data infrastructures are not co-opted and that the ecosystem is allowed to flourish with room for healthy competition.

5. **Restrict the use of DEPA for profiling:** DEPA will facilitate an increased availability of data pertaining to user citizen behaviour across areas such as finance and health, which is attractive for financial institutions looking to underwrite access to credit or insurance. This may incentivize a push for data sharing to become mandatory for access to services that have the potential to exclude those who are 'data poor' or more comfortable with physical documentation. The use of data for financial profiling should be tightly controlled, given the potential for these techniques to carry forward biases based on historical inequities.