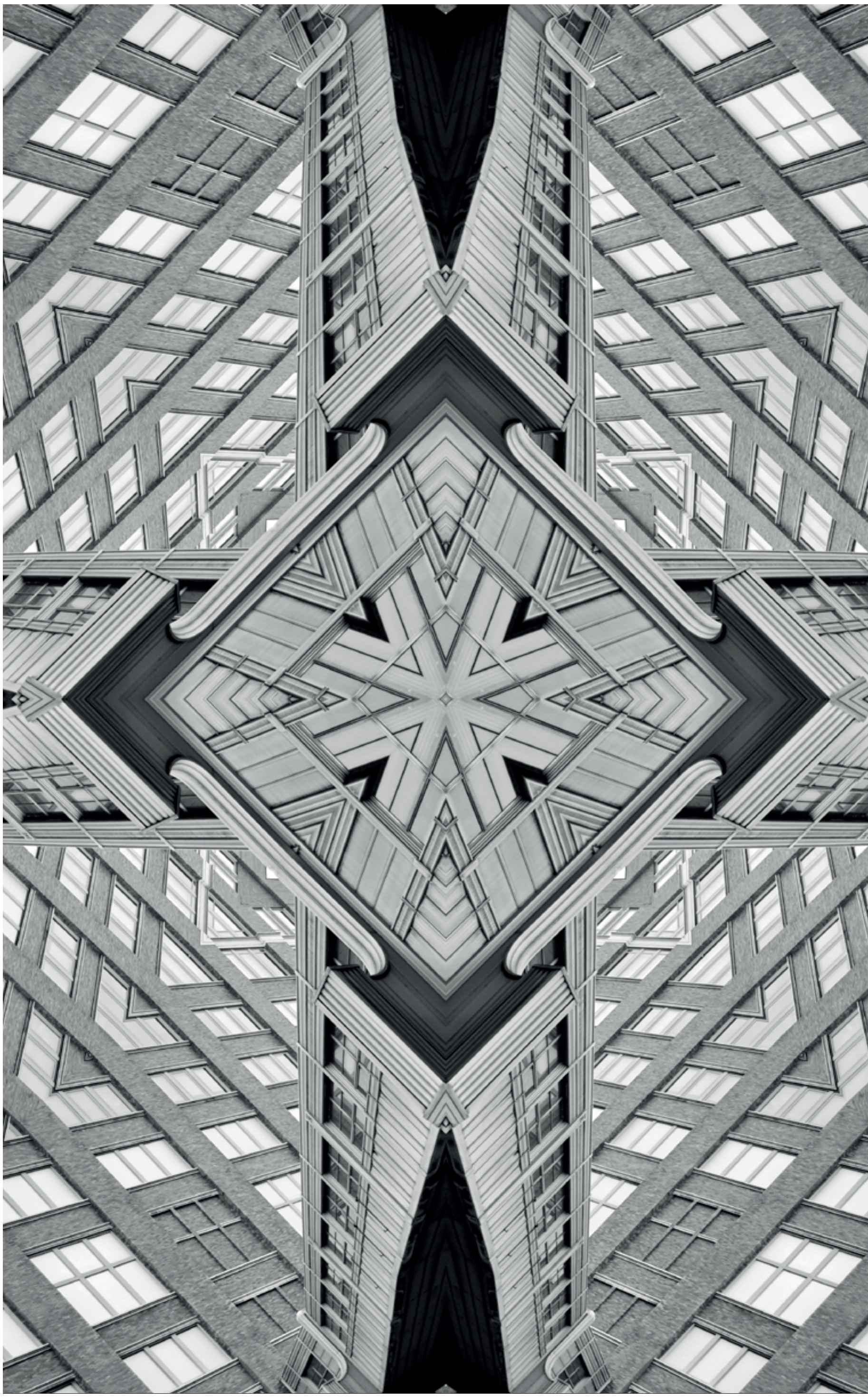
OBSERVER RESEARCH FOUNDATION

Issue Brief

ISSUE NO. 487
AUGUST 2021



Data Empowerment and Protection Architecture: Concept and Assessment

Vikas Kathuria

Abstract

Free flow in data can unlock huge social and economic value in user data that is usually locked in silos. With this motivation, Data Empowerment and Protection Architecture (DEPA), a public-private endeavour, is being developed in India as a template for users to access and share their data on their terms. Not only does this form of data sharing promote competition, but it fosters innovation as well. This brief dissects the conceptual layers of DEPA and explains its building blocks, and offers recommendations on the legal, commercial and institutional aspects of the framework to improve its workability.

Attribution: Vikas Kathuria, "Data Empowerment and Protection Architecture: Concept and Assessment," *ORF Issue Brief No. 487*, August 2021, Observer Research Foundation.

Introduction

Aadhar[a] and Unified Payments Interface (UPI)[b] services, both part of IndiaStack,[c] are primary examples of Application Programming Interface (API)-based[d] products that in the past few years have revolutionised user authentication and real-time digital payments, respectively, in India. In this series, Data Empowerment and Protection Architecture (DEPA) is being seen as the next techno-legal solution that will empower users by giving them control over their data, allowing them seamless sharing and therefore inducing competition and enabling new services.

DEPA is a joint public-private effort for an improved data governance approach.[1] It creates a digital framework that allows users to share their data on their own terms through a third-party entity, Consent Mangers.[2] It went live in the financial sector in 2020 under the joint leadership of the Ministry of Finance, the Reserve Bank of India (RBI), Pension Fund Regulatory and Development Authority (PFRDA), Insurance Regulatory and Development Authority (IRDAI), and Securities and Exchange Board of India (SEBI). DEPA is being tested in the health sector,[3] as well as others.

It has been designed as a mechanism that goes beyond data protection through a Privacy Enhancement Technology (PET) to ensure data empowerment by facilitating smooth and secure data flow. The Data Protection Committee Report had supported the idea of a Consent Dashboard that would let a data principal have access to a dashboard operated by a third party to keep track of consent to different fiduciaries.[4] The RBI-supported Account Aggregator (AA) mechanism is one such dashboard, following the DEPA model, that allows a user to access their financial data at one place.[5] This framework was envisioned by the RBI in 2015 as a service to offer consolidated views to a user of their accounts across

[a] Aadhar is the Unique Identification (UID) number issued to all residents of India that serves as proof of identity and proof of address. See: https://www.uidai.gov.in/16-english-uk/aapka-aadhar/14-what-is-aadhar.html

[b] Unified Payments Interface (UPI) is an instant payment system developed by the National Payments Corporation of India (NPCI), an RBI-regulated entity. UPI is built over the IMPS infrastructure and allows users to instantly transfer money between any two parties' bank accounts. See: https://www.npci.org.in/what-we-do/upi/faqs#:~:text=Unified%20Payments%20Interface%20(UPI)%20is,any%20two%20parties'%20bank%20accounts.

[c] IndiaStack is a set of APIs that allows governments, businesses, startups and developers to utilise a unique digital infrastructure aimed at "presence-less, paperless, and cashless service delivery." See: https://www.indiastack.org/about/

[d] APIs (Application Program Interface) are tools that developers and programmers use to create software. They work as a back-and-forth form of information between the user and the institution you are interacting with. For example, when you buy a ticket online, APIs send the information (e.g., credit card details) to the company to transform the data into the final ticket. See: https://apifriends.com/api-management/api-industry-standards/

financial institutions. It then evolved into a system for consent-based data sharing between financial sector entities.[6] Similar structures are under development in the health and telecommunication sectors.

Another manifestation of DEPA has begun with the Open Credit Enablement Network (OCEN) in the financial sector.[7] OCEN allows a user to share with a potential lender their financial data from various sources, such as the Goods and Services Tax (GST) record from the GST system, bank statement from the bank, and the Tax Deducted at Source (TDS) return from the income tax system—to prove their creditworthiness without having to show assets. This data sharing happens through a third-party Consent Manager (CM) through the use of APIs. The lender in turn decrypts this data and uses their own algorithms to assess the creditworthiness and either approve or reject a loan application. This way, a small business, who may not have adequate assets, uses its own data to get a loan.[8]

In principle, this possibility was available before DEPA as well. But the user would have to deal with data controllers separately. This process was time-consuming and thus suboptimal. Additionally, data formats are varied and may not always be interoperable. OCEN now makes this process digital, swifter and most importantly, secure, by letting the user decide the terms of data sharing.

This brief analyses the DEPA framework, which although in its early stage, can unlock benefits in personal data sharing. It offers recommendations for improving the workability of the model. The rest of the brief explains DEPA conceptually; analyses data portability and data interoperability—two building blocks of DEPA; analyses the salient aspects of DEPA; and offers suggestions for improvement.

> “DEPA will empower users in India by giving them control over their data, therefore inducing competition and enabling new services.”

DEPA: Concept and Framework

Value in data sharing

Data is reusable and usually non-rivalrous,[9] in that it can be reused without affecting the previous user. Processing of data in combination with data analytics (software), generates information of social and economic value. It can help boost productivity and improve or foster new products, processes, organisational methods and markets.[10]

In principle, therefore, free-flow in data can unlock products and services that are beneficial for society and the economy. The Organization for Economic Cooperation and Development (OECD) estimates that data access and sharing can generate social and economic benefits worth between 0.1 percent and 1.5 percent of gross domestic product (GDP) in the case of public-sector data, and between 1 percent and 2.5 percent of GDP when including private-sector data.[11]

A user generates swathes of data in the digital world. Typically, user data sits in silos and sharing of data with others is difficult. Data clubbing and sharing have a huge role to play in promoting competition and innovation. For instance, clubbing of financial data from various service providers may reveal unique information about a user. Aside from proving the creditworthiness of a user, this information may facilitate a financial planner to offer optimal products. In the health sector, data sharing would mean that a patient can share their test and treatment records with a new hospital in real-time. This cuts down the time taken to offer medical assistance.

Cross-sectoral data sharing can also be employed to offer innovative services. Sharing data from wearable health devices with insurers can reveal real information about a user and can help design custom products.

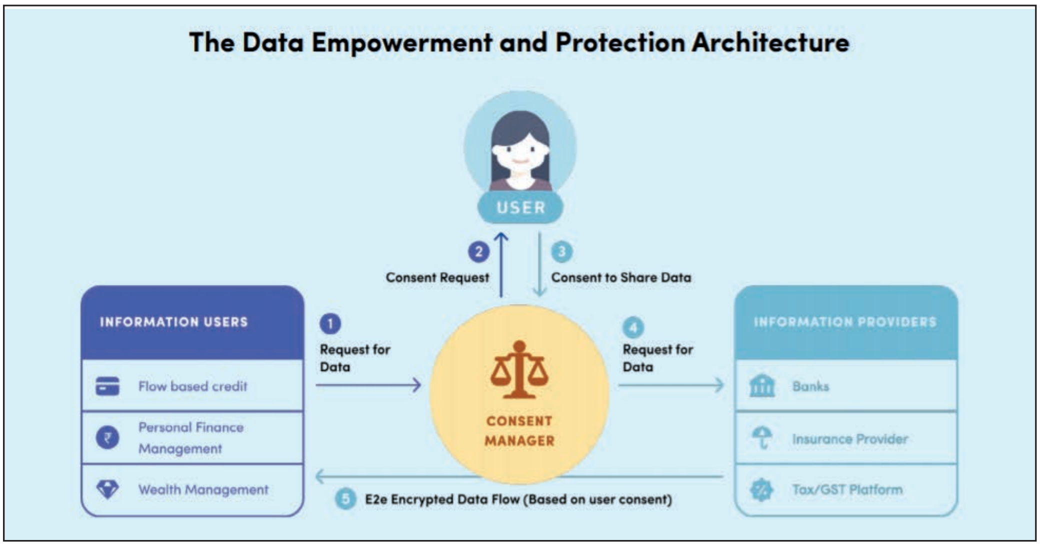
> “In principle, free-flow in data can unlock products and services that are beneficial for society and the economy.”

The DEPA framework to facilitate data-sharing

DEPA is built on the premise that users have control over their data, which can be used for their empowerment. It is an architecture that lets users securely access their data and share the same with third parties.[12]

Users interact with data controllers through Consent Managers by providing their consent to access a specific kind of data with data users through standardised APIs.[13] Previously, the same option was cumbersome in that it involved bulk printout notarisation and physical submission, screen scraping, username/password sharing, and terms and conditions forms providing blanket consent.[14]

Figure 1



Source: https://niti.gov.in/sites/default/files/2020-09/DEPA-Book_0.pdf

An early example of DEPA is the Account Aggregator (AA) framework in the financial sector spearheaded by the RBI.[15] AAs are Non-Banking Financial Companies (NBFCs) that act as a digital platform where users can see their entire financial data from different entities called Financial Information Providers (FIPs), such as banks, mutual funds, insurance provider and tax/GST platform. It is also where they can consent to share the data with a Financial Information User (FIU),such as personal finance management, wealth management and robo advisers.[16] In the present scheme of AA, FIUs can use only asset-based data such as bank accounts, deposits, mutual funds, insurance policies, and pension funds.[17] To manage and improve this architecture, a Collective of Account Aggregator ecosystem has been set up as a non-government, private limited company, known as Sahamati.[18]

One immediate benefit of the DEPA framework is that it encourages competition among players. Consent managers, as the existing AA structure suggests, will sit between multiple data fiduciaries and data users. Instead of requesting data portability, this data-sharing architecture allows the flow of data from multiple controllers to the desired destination. At the same time, the user can determine the terms of data flow such as the scope and duration of data sharing, and can revoke the same.[19]

Key to this architecture is that it separates consent collection from data flow:[20] "consent to collect" by a data user does not include "consent to share". The CMs are data-blind themselves, as they do not store the data of users and merely act as a conduit. This means that a Consent Manager does not "determine… the purpose and means of processing of personal data" and is therefore not a 'data fiduciary'.[21] Additionally, a data controller does not get to know the identity of the data user. Moreover, the data flowing through the architecture is encrypted and can be decrypted only by the FIU for which it is intended.[22]

Is DEPA a new solution?

Is DEPA unique? The concept of Consent Managers is akin to that of Personal Data Store (PDS) or Personal Information Management System (PIMS), which has been under development in the European Union (EU) for some time. PIMS is a technology that enables individuals to gather, store, update, correct, analyse, and/or share personal data; it allows for the ability to grant and withdraw consent to third parties for access to data about oneself.[23] Thus, PIMS acts as a data dashboard by either repatriating all the data on the PIMS (called warehousing) or keeping the data distributed but using the data integration methodology to interface with the different data sources (called the mediator approach).[24] Some examples of PIMS are Dataswift/Hub of All Things, Mydex, DigiMe, or CitizenMe, and Databox and Solid.[25]

> "Key to DEPA is that it separates consent collection from data flow: 'consent to collect' does not include 'consent to share'."

Users' data that resides with several services gets replicated inside PIMS, which provides the ability to exert control over this data. For instance, a user can share this data with a competing service provider.[26]

To be sure, PIMS does not always act as data stores. In an alternative model, PIMS creates a logical link among users' data, which may stay with various service providers.[27] Thus, in some form, a PIMS can resemble the DEPA framework. Where PIMS stores data, an obvious downside is that a breach may compromise all data related to a user.

Interestingly, the PIMS model allows access to different types of data, for instance, the combination of medical data with dietary patterns, or bank statements with shopping history to analyse health or spending.[28] This may reveal unique information about the user and thus may lead to new business models.

Data transfer between service providers takes place through APIs, a technical interface for accessing data by third-party software.[29] The seamless integration of data requires a common set of de facto standards and high-performance APIs to link various services and users' data. However, such common standards are lacking at present.[30]

On a conceptual level, both PIMS or CMs are a type of intermediary in the form of a multi-sided market connecting individuals offering their data for (re) use organisations wishing to (re)use this data and organisation that hold the data.[31]

Similar models

The structure of DEPA in the financial sector approximates that of Open Banking in the United Kingdom (UK), enabled by the PSD2 Directive[32] in 2018. Open Banking mandates the UK's nine biggest banks – HSBC, Barclays, RBS, Santander, Bank of Ireland, Allied Irish Bank, Danske, Lloyds and Nationwide – to release their data in a secure, standardised form, so that it can be shared more easily between authorised organisations online.[33]

Not only does Open Banking let a user see all their accounts in one place and compare the offerings (such as offered interest rates), but it also allows them to prove their creditworthiness by allowing the sharing of banking transactions data with third-party lenders. This also results in the creation of new financial products. These new financial products and services are offered by entities regulated by the Financial Conduct Authority (FCA) and European equivalents.[34]

To implement Open Banking in the UK, the Competition and Markets Authority (CMA) established the Open Banking Implementation Entity (OBIE), governed by the CMA and funded by the UK's nine largest retail-banking firms.

The OBIE has designed APIs to enable interoperability between different service providers.[35] Just like DEPA, Open Banking was designed to bring more competition and innovation to financial services.[36]

Since 2018, 300 fintech and innovative providers have joined the open banking ecosystem in the UK.[37] Further, more than 2.5 million UK consumers and businesses are now using open banking-enabled products to manage their finances, access credit, and make payments.[e,38,39]

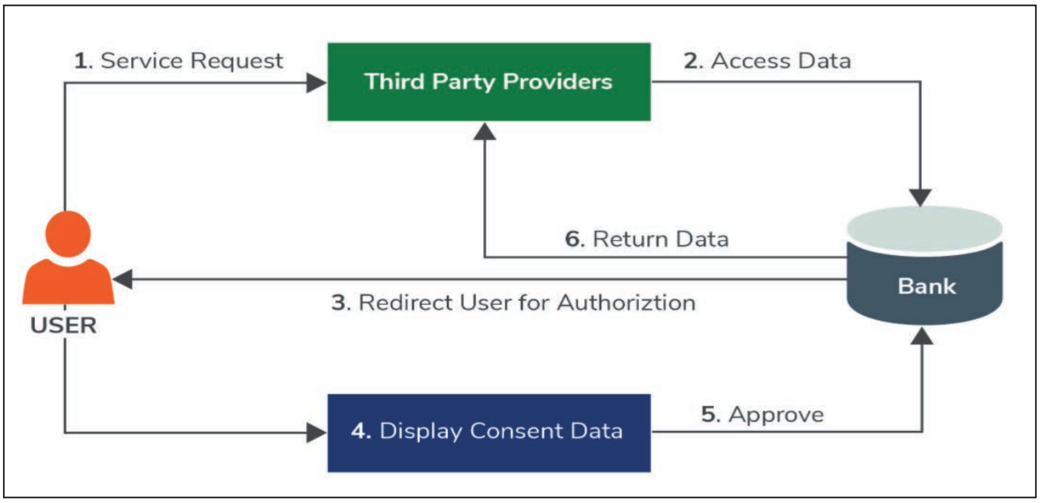
The Indian Account Aggregator model is also an example of open banking.[40] In both the AA and the UK Open Banking frameworks, there is no need to share passwords or login details to allow screen scraping. Instead, sharing of data happens under the full control of the user and as per their terms. A crucial difference is that the DEPA model tasks Consent Managers to be intermediaries;[41] such an intermediary is absent in the Open Banking model. One immediate benefit of the DEPA model is that different data providers do not need to contact the user separately. Instead, once the user provides their consent to a CM, it is the CM who connects with different types of data providers. In a paper analysing DEPA, the government think-tank NITI Aayog envisions that "[i]n the future…[CMs]could also help individuals and small businesses protect and enforce their data rights."[42]

As a dashboard, CMs would also "enable data principals to keep track of consent for processing in real time and allow them to operationalise the right accorded to them under the data protection law."[43] Moreover, the AA app can show a user all the consents given, the revoked consents, and a log of all data requests made by the FIU. A user can revoke consents through this AA app.[44]

In the same paper, NITI Aayog observes that DEPA is a superior model compared to Open Banking as it segregates the institution collecting the data (such as banks) and the institution collecting consent (in this case, CMs).[45] Whereas, in the case of Open Banking, data providers (banks) work directly with Account Information Service Providers (AISPs) (data users) to gather individual consent. The desegregation of collection and consent, the Paper observes, "may not work to address India's scale and diversity"[46] The paper, however, does not explain it.

[e] The Open Banking webpage lists 109 open banking apps that provide a range of solutions, essentially based on open banking, to users. There is a sufficient degree of competition in this market.

Figure 2



Source: https://wso2.com/ibrary/articles/2019/09/consent-management-for-open-banking/

Privacy by design

Earlier solutions that promised welfare-enhancing services, like Aadhar, have been put to doubt around their ability to ensure privacy and fairness. Some such solutions even had to be abandoned altogether as they were unable to deal with these risks.[47] Even as DEPA does not involve aggregated data of users, a framework that is weak on privacy would likely fail to inspire user trust.

Behind the concept of 'privacy by design' lies the idea that data protection in data processing procedures is best adhered to when it is already integrated into the technology as it is being created.[48] It requires ensuring privacy through technical and organisational means, from the design stage and throughout the life cycle.[49] Thus, privacy by design goes beyond encryption: it must ensure that privacy is embedded into the design, operation, and management of information communication technologies and systems. [50]

DEPA, illustrated in the AA model, can go beyond the requirement of user authentication to ensure Privacy by Design. In the AA model, the RBI has mandated that no financial information of the customer accessed by the Account Aggregator from the financial information providers will reside with the Account Aggregator.[51] Equally important, the Account Aggregator will not use the services of a third-party service provider for undertaking the business of account aggregation.[52]

Advantages of DEPA

Reduction in transaction cost and increased competition are not the only benefits of DEPA. PIMS or CMs can also be viewed as a kind of Privacy Enhancing Technologies (PETs) that aim at employing technological solutions to ensure user privacy and security.[53] PETs safeguard privacy by allowing users to decide, amongst other things, what information they are willing to share with third parties such as online service providers, under what circumstances that information will be shared, and what the third parties can use that information for.[54] DEPA as a technological solution meets these criteria. Another advantage of this architecture is that it prevents the data holder from knowing the identity of the data requestor.[55]

This architecture can usher in innovative solutions in digital markets. For instance, this author and Lai have looked at the need and ways to port user reviews from one platform to another using the PIMS framework. User reviews are a type of reputation management and an easy transition of reviews from one platform to another may facilitate competition. To this end, PIMS may act as an intermediary.[56]

> “Data protection in data processing procedures is best adhered to when it is integrated into the technology as it is being designed.”

Data Portability

The most fundamental building block of DEPA is the concept of data portability. As mentioned briefly above, data, in principle, is non-rival resource. Data portability is a right that allows users to request a data holder to share their data with a third party.

In current digital markets, a small number of firms hold a large part of users' data. The technological and economic characteristics of digital businesses, most notably network effects, lead to market concentration.[57] Data portability is a means to ensure that users do not get locked in. While a user could request portability from firm A to firm B, the DEPA architecture allows them to request portability from multiple firms at the same time. In banking and healthcare, for instance, data can create value for users as network effects may not be decisive to the success of a bank unlike the case of data-driven businesses such as social media or online search. In a short span of time, therefore, an innovative firm can make space for itself. In turn, it is not clear how efficient DEPA could be in fostering competition in a market that experiences strong network effects.

Data portability can also facilitate completely new businesses in digital markets. For instance, data from social-media platforms like Facebook, WhatsApp, Instagram and Twitter can be clubbed to form a completely new platform. So while horizontal interoperability—i.e., portability between two similar services—is unviable, this new form of competition is possible.

This form of data sharing also has the potential to counter network effects in the established market by facilitating new business models that may challenge the old ones. For instance, the app WeChat combines social-media messaging and calling apps, WeChat localisation, QR code scan, search engine, a news feed, and e-wallet, among many other services that it offers.[58]

> “Under DEPA, data is portable: a data holder can share their data with a third party.”

The Building Blocks of DEPA

Data interoperability

DEPA is a solution that integrates data providers with data users. In general, lack of data interoperability due to non-standardisation impedes the growth of services that require data sharing.[59] In DEPA, different agents can communicate with each other by effectively integrating datasets through the use of APIs.

In the past too, API-enabled services such as the layered digital service and open API framework known as IndiaStack enabling verifiable identity (Aadhar), eKYC data sharing, and an interoperable Unified Payments Interface (UPI) have provided crucial digital tools to facilitate easy transactions.[60]

In general, non-standardised APIs is a challenge faced by digital solutions. Non-standardisation impedes interoperability and thus fractures a digital service. For DEPA's Account Aggregator architecture, the RBI took the initiative to standardise APIs.[61] These are open APIs for data sharing that allow a new consent manager to "plug in" to a common sharing system rather than having to build bilateral relationships with information providers to access data.[62]

> "DEPA is a solution that integrates data providers with data users."

Legal Basis

In banking, the RBI has issued a Master Directive to create Account Aggregators.[63] For other sectors where DEPA will be used, wider adoption of the model would depend upon the legal rights of a user. The DEPA model should have an overall legislative mandate if it is to be adopted across sectors.

The current legislative framework that governs user data in India is the Information Technology (IT) Act, 2000 that requires user consent before any entity shares 'sensitive data' with third parties.[64] It, however, does not provide for a framework that recognises users' control over their data and mandates data portability. That framework is present in the draft Personal Data Protection Bill, 2019. The most fundamental legal basis of DEPA is the right to data portability enshrined in Sec 19 (1) of the Bill. Data access rights are crucial too, though they do not mandate that data be returned in a machine-readable format, which the right to data portability does.[65] Section 19 (1) of the draft Bill states:

(1) Where the processing has been carried out through automated means, the data principal shall have the to—

> (a) receive the following personal data in a structured, commonly used and machine-readable format…

Further, Sec 23(3) of the draft PDP Bill provides: "[T]he data principal may give or withdraw his consent to the data fiduciary through a consent manager.". In turn, a consent manager has been defined as "a data fiduciary which enables a data principal to gain, withdraw, review and manage his consent through an accessible, transparent and interoperable platforms"[66] Together, Sections 19 (1) and 23 (3) of the draft PDP Bill form the legislative mandate upon which the DEPA framework will rest. Bypassing this mandate, until the Bill becomes law, through sector-specific legislation is cumbersome and would delay the advantages of the DEPA framework.

DEPA is aimed at giving more control to users over their data. However, the draft PDP Bill makes no explicit declaration. In contrast, the EU General Data Protection Regulation (GDPR) explicitly recognises users' control over their data.[67] In effect, however, the draft PDP bill recommends similar rights as enshrined in the GDPR. Thus, user control in India will be a natural corollary of such rights.

Passing the PDP Bill, therefore, is an imperative. Giving DEPA legal sanction would ensure that market players, independent of sectoral regulators, can innovate and build upon the techno-legal infrastructure enshrined in DEPA.

The inclusion of 'inferred data'

Derived or 'inferred data'[68] is the result of further analyses through data processing, e.g. by a personalisation or recommendation process, or by user categorisation or profiling.[69] Article 29 Data Protection Working Party[f] states a credit score or the outcome of an assessment regarding the health of a user is a typical example of inferred data.[70] Inferred data falls outside the scope of data portability in the EU, as such data is not "provided by" a user or results from the observation of an individual's behaviour.[71]

It has been argued that the portability right in India as enshrined in the draft PDP Bill, 2019 also applies to profile information, even if the data may be inferred.[72] This broad mandate to share inferred data too may need be thought through more carefully. In many cases, sharing inferred data may create a disincentive for the incumbents as inferring information requires investment and skills.

Further, some caution must be excercised too, with respect to 'derived data' (data with masked personally identifiable information but could reveal confidential data of a company). It should be ensured that proprietary company algorithms or techniques should not be revealed through data sharing.[73]

In view of the above, the application of DEPA to different data sub-categories needs to be discussed and debated before any guidelines are adopted.

> "Caution must be exercised around 'inferred data', or data that results from further analyses by data processing."

[f] This Working Party was set up under Article 29 of EU Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

Allowing incumbents to be Consent Managers

Is there a problem if an Account Aggregator also happens to be a Financial Information User (FIU) or a Financial Information Provider (FIP)? Incumbents and integrated firms may not have the right incentives to allow switching. In general, it is in the commercial interest of incumbents to prevent the switching of users. Even if users are granted such a right, the design of tools such as the app may be in a way that makes switching difficult in practice. In the DEPA framework, a CM may charge less to its own firm seeking data access. As conglomerate or vertically integrated business models are common in digital markets, the likelihood of such a practice increases.[74]

While the AA framework mandates Aggregators to be 'data blind', in other sectors, especially where the architecture evolves independent of the sectoral regulator, the DEPA framework can follow that of Personal Data Stores (PDS). This means data will reside with them. This may create problems if the same entity is present in a vertical that seeks access to data. The dual role of a platform has been a cause for self-preferencing in digital markets.[75] Additionally, in such cases a CM (resembling a PDS) may downgrade the quality of data to competitors.

The RBI prescribes that an Aggregator shall not undertake any other business other than the business of an account aggregator.[76] This is a step in the right direction and should be a general standard in the DEPA framework.

Institutional Architecture

DEPA is essentially a personal data-sharing framework that requires an expert body, which understands the legalities and technical nuances involved in personal data sharing. Thus, DEPA as a general architecture should be governed and regulated by the proposed Data Protection Authority (DPA) under the draft PDP Bill, not by a sectoral regulator unless an issue falls under the expert remit of the regulator. For instance, it has been suggested that the RBI should not regulate the processing and sharing of personal information unless it is directly related to the provision of financial services.[77] The involvement of sectoral regulators in data sharing can also lead to turf wars.

Moreover, when data from two different sectors are involved, the sector-specific regulator will have even more difficulties. For instance, health and investment data can together reveal better insights about a user's creditworthiness. An overlap in jurisdiction may arise if a product falls at the intersection of the two sectors.

The role of sector regulators cannot be completely obliterated, however. As discussed earlier, standardised APIs are crucial to ensuring smooth data flows. The RBI took the lead to promote standardised APIs in the financial sector. Markets or specific sectors cannot be trusted completely to come up with standardised APIs. Indeed, industry-based Standard Setting Organizations (SSOs) are best placed to lead standardisation as they have the requisite information. However, sectoral regulators cannot completely take the back seat.[78] For instance, market leader incumbents that have data advantage and are part of SSOs will have incentives in impeding standardisation, as this will perpetuate their market position despite a clear mandate of data sharing.[79]

A critical issue is the governance and regulation of the DEPA framework. While both data providers and data users are fiduciaries and thus come within the purview of the PDP Bill, Consent Managers fall outside the Bill as they do not hold user data. In such a scenario, self-regulation or industry-based standards could provide guidance.

Conclusion

Vikas Kathuria *is a Fellow, Observer Research Foundation, New Delhi; Affiliated Research Fellow, Max Planck Institute for Innovation and Competition, Munich. The author is grateful to Arun Sukumar for very helpful discussions. All views and errors are author's alone.*

DEPA promises to be the techno-legal solution that can unlock value in data sharing by giving users more control over their data. This control not only results in increased competition but also fosters innovation. This brief aimed to critique this architecture in its early days to offer suggestions that can improve its workability.

Although DEPA is not a completely new solution, as similar architectures in the form of PIMS or PDS are evolving in the EU, the model needed unpacking because of its technological and legal complexity. Thus, the brief first examined these layers to reveal the conceptual framework behind the architecture. While DEPA can be compared to the Open Banking model in the UK, what sets it apart is the involvement of a Consent Manager that segregates consent and data flow.

The brief then explained the two building blocks of DEPA: data portability and data interoperability. Together these two parts enabled the scrutiny of legal, commercial and institutional aspects of this framework in the last part of the brief.

The broader legislative mandate behind DEPA is enshrined in the right to data portability in the draft Data Protection Bill, 2019. For the widespread use of DEPA, this right should soon be concretised in the form of legislation. The brief also recommends that sub-categories of data involved in data sharing in general and also within the framework of DEPA need to be carefully deliberated. While there may be benefits in sharing of inferred data, it may adversely affect the incentives of firms that invest in inferring data. Similarly, derived data can reveal proprietary company algorithms or techniques and thus may harm a firm if shared with competitors.

Incumbents may not have the right incentives to ensure smooth data sharing, thus they should not be allowed to undertake the role of Consent Managers. Finally, the brief recommends that institutional oversight of the DEPA framework should fall under the Data Protection Authority envisioned in the PDP Bill, 2019. Sectoral regulators, however, can be involved in the standardisation of APIs where the markets cannot take the lead in the standardisations process.

There has been a recognition that DEPA is not a static policy product; rather, it is an "evolvable and agile framework".[80] This brief has attempted to inform the policy debate on DEPA by explaining the concept to the readers and offering suggestions to policymakers at the same time. Understanding the techno-legal nuances of DEPA and addressing critical issues such as cyber security and operational risks[81] merit further research and discussion.

Endnotes

[1] NITI Aayog, Data Empowerment and Protection Architecture, Draft for Discussion, http://www.niti.gov.in/sites/default/files/2020-09/DEPA-Book.pdf

[2] NITI Aayog, Data Empowerment and Protection Architecture, Draft for Discussion

[3] Edited by Chandrashekar Srinivasan, ""Health ID For Each Indian": PM Announces National Digital Health Mission", NDTV India, August 15, 2020, https://www.ndtv.com/india-news/national-digital-health-mission-pm-modi-independence-day-speech-national-digital-health-mission-to-revolutionise-health-sector-says-pm-modi-2279792

[4] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, "A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians", https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf, page 38.

[5] Hiralal Thanawala, "Here's how account aggregators share financial data of customers with banks", Money Control, December 7, 2020, https://www.moneycontrol.com/news/business/personal-finance/heres-how-account-aggregators-share-financial-data-of-customers-with-banks-6197761.html;

[6] Malvika Raghavan and Anubhutie Singh, "Regulation of information flows as Central Bank functions?: Implications from the treatment of Account Aggregators by the Reserve Bank of India", http://financelawpolicy.umich.edu/files/raghavan-singh-regulation-of-information-flows-as-central-bank-functions-implications-from-treatment-account-aggregators-india.pdf

[7] MEDICI, "India's Open Credit Enablement Network (OCEN)", February 12, 2021, https://gomedici.com/indias-open-credit-enablement-network-ocen; iSPIRT, "iSPIRT Second Open House on OCEN: Varied LSP Possibilities", August 1, 2020, https://pn.ispirt.in/tag/open-credit-enablement-network/

[8] Sunil Jain, "The West created monopolies, we democratised data: Nandan Nilekani, co-founder, Infosys", Financial Express, May 21, 2021, https://www.financialexpress.com/industry/the-west-created-monopolies-we-democratised-data-nandan-nilekani-co-founder-infosys/2225178/

[9] Charles I. Jones and Christopher Tonetti, "Nonrivalry and the Economics of Data", August 2019, Stanford GSB, Working Paper No. 3716, https://www.gsb.stanford.edu/faculty-research/working-papers/nonrivalry-economics-data

[10] The OECD, "Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies", page 16, https://www.oecd.org/publications/enhancing-access-to-and-sharing-of-data-276aaca8-en.htm

[11] The OECD, Enhancing Access to and Sharing of Data, page 11.

[12] NITI Aayog, Data Empowerment and Protection Architecture, Draft for Discussion

[13] NITI Aayog, Data Empowerment and Protection Architecture, Draft for Discussion

[14] NITI Aayog, Data Empowerment and Protection Architecture, Draft for Discussion

[15] The RBI issued the Account Aggregator (Consent Managers) Directions on September 02, 2016, which was last updated on November 22, 2019, see https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10598&Mode=0

Endnotes

16 Sahmati , Sahamati – Collective of the Account Aggregator Ecosystem, https://sahamati.org.in/; for the use cases of the AA model see, BG Mahesh, " Use Cases For Account Aggregator Framework", Sahamati, 5th December 2020, https://sahamati.org.in/blog/use-cases-for-account-aggregator-framework/

17 Sahamati, Frequently Asked Questions, https://sahamati.org.in/faq/

18 Sahamati, Sahamati – Collective of the Account Aggregator Ecosystem, https://sahamati.org.in/

19 BG Mahesh, " What is an Informed Consent & Consent Artefact?", Sahamati, 14th June 2020, https://sahamati.org.in/blog/what-is-an-informed-consent-consent-artefact/

20 See,MeitY, Electronic Consent Framework, Technology Specifications, Version 1.1, page 7, http://dla.gov.in/sites/default/files/pdf/MeitY-Consent-Tech-Framework%20v1.1.pdf

21 Sec 2 (13) of the PDP bill states ' "data fiduciary" means any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data."

22 Sahamati, Sahamati – Collective of the Account Aggregator Ecosystem

23 Guillaume Brochot, Julianna Brunini, Franco Eisma Rebekah Larsen and Daniel J. Lewis, "Personal Data" Stores, Cambridge Judge Business School, 2015, page 2.

24 Jan Krämer, Pierre Senellart, Alexandre de Streel, "Making Data Portability More Effective for the Digital Economy: Economic Implications And Regulatory Challenges", June 2020, CERRE, page 45.

25 Heleen Janssen, Jennifer Cobbe, Chris Norval and Jatinder Singh, "Decentralized data processing: personal data stores and the GDPR" International Data Privacy Law, 2020, Vol. 10, No. 4.

26 Serge Abiteboul, Benjamin André, Daniel Kaplan. Managing your digital life with a Personal information management system. Communications of the ACM, Association for Computing Machinery, 2015, 58 (5), pp.32-35

27 Opinion 9/2016, EDPS Opinion on Personal Information Management Systems: Towards more user empowerment in managing and processing personal data, 20 October 2016, page 6.

28 Heleen Janssen, Jennifer Cobbe, Chris Norval and Jatinder Singh, "Decentralized data processing: personal data stores and the GDPR", p 362.

29 Jan Krämer, Pierre Senellart, Alexandre de Streel, "Making Data Portability More Effective for the Digital Economy: Economic Implications And Regulatory Challenges"

30 Jan Krämer, Pierre Senellart, Alexandre de Streel, "Making Data Portability More Effective for the Digital Economy: Economic Implications And Regulatory Challenges"

31 Opinion 9/2016, EDPS Opinion on Personal Information Management Systems: Towards more user empowerment in managing and processing personal data, page 11.

32 See, UK Finance, " Payment Services Directive 2 and Open Banking", https://www.

ukfinance.org.uk/guidance/payment-services-directive-2-and-open-banking

33 Rowland Manthorpe, “What is Open Banking and PSD2? WIRED explains”, WIRED, April 17, 2018, https://www.wired.co.uk/article/open-banking-cma-psd2-explained

34 Open Banking, “What is Open Banking?”, https://www.openbanking.org.uk/customers/what-is-open-banking/

35 The OECD, Data portability, interoperability and digital platform competition – Background Note, DAF/COMP(2021)5.

36 Open Banking, “What is Open Banking?”

37 Open Banking, “Three years since PSD2 marked the start of Open Banking, the UK has built a world-leading ecosystem”, https://www.openbanking.org.uk/about-us/latest-news/three-years-since-psd2-marked-the-start-of-open-banking-the-uk-has-built-a-world-leading-ecosystem/

38 Open Banking, “Three years since PSD2 marked the start of Open Banking, the UK has built a world-leading ecosystem”

39 Open Banking, “Start your Open Banking Journey”, https://www.openbanking.org.uk/app-store/

40 Shri M. Rajeshwar Rao, Deputy Governor, Reserve Bank of India, discusses the AA model as an Open Banking solution in his speech, https://m.rbi.org.in/scripts/BS_SpeechesView.aspx?Id=1107

41 MeitY, Electronic Consent Framework Technology Specifications, Version 1.1

42 NITI Aayog, Data Empowerment and Protection Architecture, Draft for Discussion, page 17, also at 36.

43 NITI Aayog, Data Empowerment and Protection Architecture, Draft for Discussion, page 33.

44 Sahamati, Frequently Asked Questions

45 NITI Aayog, Data Empowerment and Protection Architecture, Draft for Discussion, page 28.

46 NITI Aayog, Data Empowerment and Protection Architecture, Draft for Discussion, page 28.

47 Prashant Agrawal, Anubhutie Singh, Malavika Raghavan, Subodh Sharma and Subhashis Banerjee, “An operational architecture for privacy-by-design in public service applications” (2020), https://arxiv.org/abs/2006.04654

48 Intersoft Consulting, “GDPR: Privacy by Design”, https://gdpr-info.eu/issues/privacy-by-design/

49 The UK Information Commissioner’s Office, “Data protection by design and default”, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/

Endnotes

50 The European Union Agency for Network and Information Security (ENISA), "Privacy and Security in Personal Data Clouds", Final Report Public, November 2016, page 16.

51 Article 5 (g) Master Direction- Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016.

52 Article 5(h) Master Direction- Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016.

53 The Royal Society, Privacy Enhancing Technologies, 21 July 2021, https://royalsociety.org/topics-policy/projects/privacy-enhancing-technologies/

54 Office of Privacy Commissioner of Canada, "Privacy Enhancing Technologies – A Review of Tools and Techniques",https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711/; see also, Data Security Council of India (DSCI), " Privacy Enhancing Technologies", https://www.dsci.in/content/privacy-enhancing-technologies

55 The World Bank, "Unraveling Data's Gordian Knot: Enabler's and Safeguards for Trusted Data Sharing in the New Economy", 2020, page 52.

56 Vikas Kathuria and Jessica C. Lai, "User review portability: Why and how?", Computer Law & Security Review Volume 34, Issue 6, December 2018, Pages 1291-1299.

57 Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, "Competition policy for the digital era", 2019, European Commision; Jason Furman, Diane Coyle, Amelia Fletcher, Philip Marsden and Derek McAuley "Unlocking digital Competition: Report of the Digital Competition Expert Panel", Crown Copyright, March 2019.

58 Emerline, " What is a Super App? Reasons for Success?", Nov 12, 2020, https://emerline.com/blog/what-is-a-super-app

59 Satchit Balsari et al, "Reimagining Health Data Exchange: An Application Programming Interface-Enabled Roadmap for India" (2018) 20 (7): July, Journal of Medical Internet Research.

60 NITI Aayog, Data Empowerment and Protection Architecture, Draft for Discussion.

61 Reserve Bank Information Technology Pvt. Ltd. (REBIT), Account Aggregator Ecosystem API Specifications, https://api.rebit.org.in/

62 NITI Aayog, Data Empowerment and Protection Architecture, Draft for Discussion

63 Reserve Bank of India, Master Direction- Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016 (Updated as on November 22, 2019).

64 Sec 72A of the Information Technology Act, 2000.

65 Janssen, H. & Cobbe, J. & Singh, J. (2020). "Personal information management systems: a user-centric privacy utopia?" Internet Policy Review, 9(4). https://doi.org/10.14763/2020.4.1536, page 12.

66 Explanation to Sec 23 PDP Bill, 2019.

67 Recital 7 & 68, the General Data Protection Regulation (GDPR).

Endnotes

68 For a taxonomy of different types of data see, OECD, "Summary of the OECD Privacy Expert Roundtable", DSTI/ICCP/REG(2014)3.

69 Article 29 Data Protection Working Party, " Guidelines on the right to data portability", 2016. https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf

70 https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdfDEPA as a framework could apply to personal data (data with personally identifying information) and to derived data (data with masked personally identifiable information but could reveal confidential data of a company). When sharing the latter, care ought to be taken to maintain a

71 Article 29 Data Protection Working Party; Article 20 GDPR: "The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided"

72 Diana Lee, Gabe Maldoff and Kurt Wimmer, "Comparison: Indian Personal Data Protection Bill 2019 vs. GDPR", IAPP, https://iapp.org/resources/article/comparison-indian-personal-data-protection-bill-2019-vs-gdpr/; Aditi Agrawal, " A lowdown on Personal Data Protection Bill 2019", Forbes India, Jan 28, 2021, https://www.forbesindia.com/article/special/a-lowdown-on-personal-data-protection-bill-2019/66037/1

73 NITI Aayog, Data Empowerment and Protection Architecture, Draft for Discussion, page 36-37.

74 OECD, Data portability, interoperability and digital platform competition – Background Note, DAF/COMP(2021)5, page 11.

75 CASE AT.39740 Google Search (Shopping) European Commision; CASE AT.40099 Google Android.

76 Sec 5 (f) Master Direction- Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016.

77 Malvika Raghavan and Anubhutie Singh, "Regulation of information flows as Central Bank functions? Implications from the treatment of Account Aggregators by the Reserve Bank of India"

78 See, Michal Gal and Daniel L Rubinfeld, "Data Standardization", (June 2019). 94 NYU Law Review (2019) Forthcoming, NYU Law and Economics Research Paper No. 19-17, Available at SSRN: https://ssrn.com/abstract=3326377 or http://dx.doi.org/10.2139/ssrn.3326377/. The authors highlight the reasons for which government in some cases can play an important role in standardization.

79 Michal Gal and Daniel L Rubinfeld, "Data Standardization"

80 NITI Aayog, Data Empowerment and Protection Architecture, Draft for Discussion

81 RBI, Opean Banking in India, Remarks by Shri M. Rajeshwar Rao, Deputy Governor, Reserve Bank of India - Wednesday, April 14, 2021 - in a webinar on Open Banking organised by Tata Consultancy Services (TCS) in association with the Embassy of India in Brazil, https://m.rbi.org.in/scripts/BS_SpeechesView.aspx?Id=1107

ORF OBSERVER RESEARCH FOUNDATION

Ideas . Forums . Leadership . Impact

20, Rouse Avenue Institutional Area,
New Delhi - 110 002, INDIA
Ph. : +91-11-35332000. **Fax :** +91-11-35332005
E-mail: contactus@orfonline.org
Website: www.orfonline.org