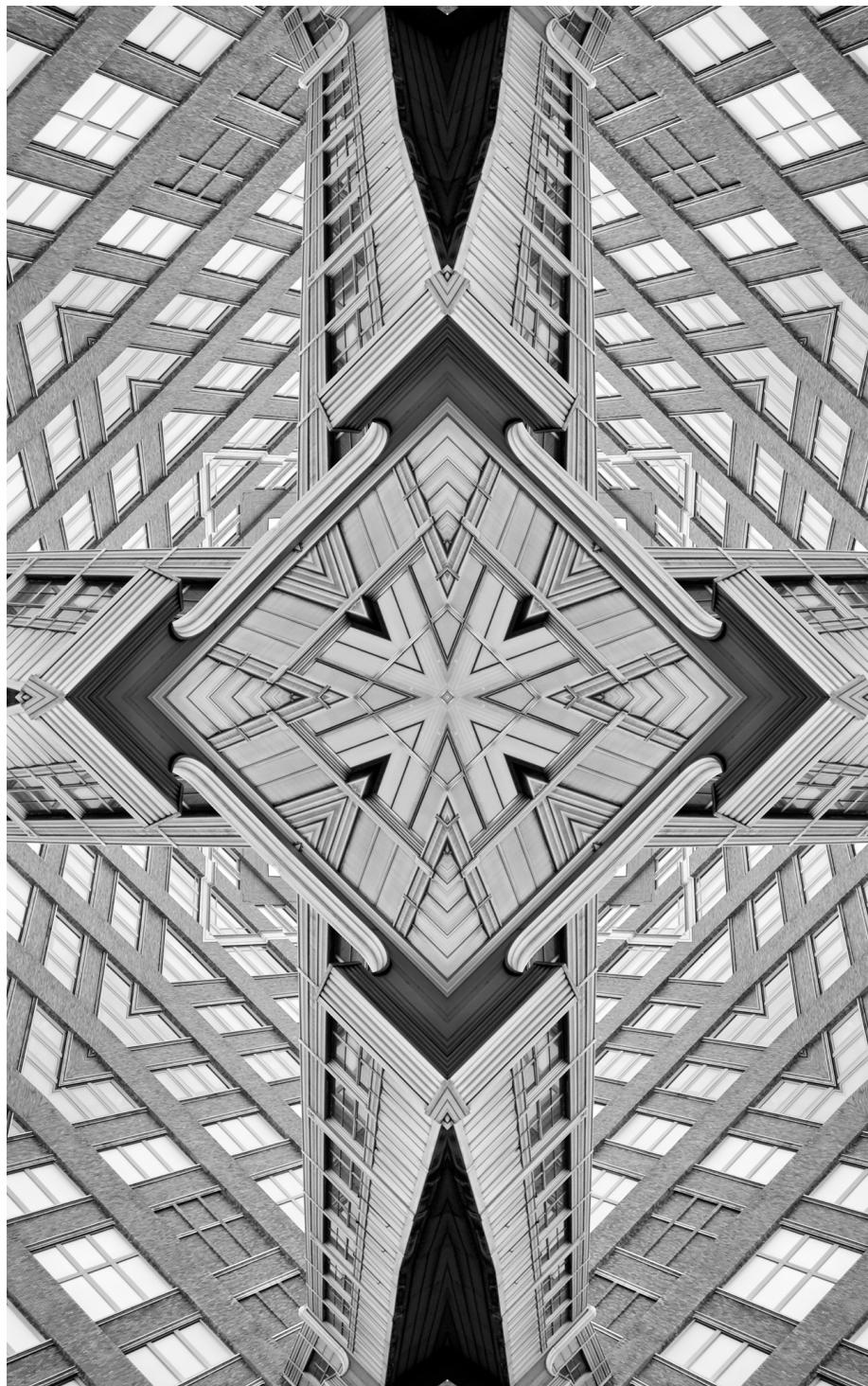


# Issue Brief

ISSUE NO. 811  
JUNE 2025



© 2025 Observer Research Foundation. All rights reserved. No part of this publication may be reproduced, copied, archived, retained or transmitted through print, speech or electronic media without prior written approval from ORF.

# India's Journey in Open Banking: Consent, Control, and Connectivity

**Sauradeep Bag**

## **Abstract**

As data drives technological innovation in finance, open banking has gained global relevance. India has advanced in this domain through initiatives like the India Stack, as well as frameworks such as the Data Empowerment and Protection Architecture (DEPA) and the Account Aggregator (AA) framework. Additionally, the Digital Personal Data Protection (DPDP) Act is increasingly shaping India's open banking landscape. Given the importance of data privacy and security, it is important to assess India's current standing in open banking. This brief explores India's progress, key challenges, and how it compares to countries that lead the world in implementing open banking frameworks.

# Introduction

‘Open banking’<sup>1</sup> is a financial paradigm that enables the sharing of customer-authorised data between banks and third-party providers through the use of secure Application Programming Interfaces (APIs), with data privacy at its core. India is developing its open banking ecosystem through advances in digital infrastructure, regulatory frameworks, and data governance. As the landscape evolves, a number of initiatives are reshaping the access and sharing of financial data.

The ecosystem rests on two fundamental principles: empowering users with greater control over their data, and preventing misuse by data recipients. Given these priorities, data privacy becomes a pillar of the framework. To understand the evolution of open banking in India, it is essential to examine the country’s approach to data privacy and how it shapes the current landscape of open banking. Understanding this relationship provides insights into both the regulatory framework and the broader implications for financial innovation and user protection.

India's path to a robust data protection and privacy framework has witnessed milestones, culminating in the enactment of the Digital Personal Data Protection (DPDP) Act, 2023.<sup>2</sup> The process began with the creation of the Justice A.P. Shah Committee<sup>3</sup> in 2015, whose report highlighted the need for comprehensive data privacy measures. In 2017, the Justice Srikrishna Committee<sup>4</sup> was tasked with drafting the country's first dedicated data protection law. Their recommendations laid the groundwork for the DPDP Act.

India's initial approach to data protection was characterised by straightforward principles outlined in the Information Technology Act, 2000<sup>5</sup> and its subsequent amendments. The 2017 Supreme Court ruling in *Justice K.S. Puttaswamy (Retd.) v. Union of India*<sup>6</sup> marked a turning point, as it recognised privacy as a fundamental right under Article 21 of the Constitution. The decision ignited widespread debates around Aadhaar and privacy, coinciding with global developments such as the introduction of the General Data Protection Regulation (GDPR) in Europe,<sup>7</sup> which set a gold standard for data protection.

While the GDPR's stringent regulations are argued to have strengthened incumbency among established players in Europe,<sup>8</sup> the rapid growth of India's digital public infrastructure (DPI) necessitated a regulatory framework that protects individual rights while fostering innovation and competition in the tech sector. The development of the Data Empowerment and Protection Architecture (DEPA) reinforces India's commitment to user empowerment, finding parallels to the principles found in the GDPR. It establishes a framework that recognises individuals as the owners of their data, emphasising that entities utilising such data must do so in a responsible and transparent manner.

The DPDP Act marks the most comprehensive articulation of these principles yet, establishing a robust legal framework for data protection. The Act seeks to empower individuals with greater control over their personal data while holding organisations accountable for their use. As the law takes effect, India seeks to balance technological innovation with stringent privacy safeguards, emphasising the importance of informed consent and protection against misuse.

## **The Data Empowerment and Protection Architecture (DEPA), 2020**

The DEPA<sup>9</sup> developed by NITI Aayog in 2020, aims to enhance individual control over personal data while ensuring secure data sharing. It marks a shift from an organisation-centric model to one centred on individual empowerment and consent.

At its core, DEPA facilitates a consent-based data-sharing mechanism that allows individuals to decide how their personal information is used and shared with third parties. This is enabled by Consent Managers—intermediaries that help users manage their consent preferences. They ensure that consent is free, informed, specific, clear, and revocable, thereby enhancing transparency in data transactions.

DEPA also emphasises interoperability, enabling seamless data sharing across various sectors, including financial services, healthcare, and e-commerce. By allowing individuals to leverage their digital footprints, DEPA aims to improve access to essential services like loans or telemedicine. This interoperability reduces reliance on outdated practices like screen scraping, which often compromise security and efficiency. DEPA is also designed as an evolvable framework—i.e., it can adapt to technological advancements and regulatory shifts. This flexibility is crucial in a dynamic digital landscape where data privacy concerns are paramount.

Ultimately, DEPA seeks to empower individuals with the tools to access, control, and selectively share their personal data. By operationalising secure and standardised data sharing, it strengthens individual rights and supports a more inclusive digital economy in which all citizens can benefit from their data.

### **DEPA and DPDP Act: Financial Data Governance**

Globally, data privacy frameworks rest on certain fundamental principles that ensure responsible data management. One such principle is purpose specification, which requires that personal data be collected for well-defined, explicit, and legitimate purposes. Organisations must disclose the purpose at the point of collection and ensure that the information is used solely as intended, thereby reducing the risk of misuse.

Another pillar is data minimisation, which requires collecting and processing only the personal data strictly necessary for a given purpose. This reduces unnecessary exposure and strengthens privacy protection. Equally important is data retention or storage limitation, which emphasises that personal data should not be kept for an indefinite period. Organisations must establish clear retention policies to delete or anonymise data once it has served its original purpose. Together, these principles curb excessive data collection and misuse, reinforcing trust in digital ecosystems while balancing technological progress with individual rights.

‘The Master Direction - Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016’, issued by the Reserve Bank of India (RBI),<sup>10</sup> establishes the regulatory framework for Account Aggregators (AAs) in India. These entities, classified as a type of Non-Banking Financial Company (NBFC), serve as intermediaries for the secure, consent-driven exchange of financial data. Unlike conventional NBFCs, AAs neither provide loans nor conduct financial transactions. Instead, they facilitate data sharing between Financial Information Providers (FIPs)—which include banks, NBFCs, and mutual funds—and Financial Information Users (FIUs), such as lenders, wealth managers, and fintech firms. The AA framework operates on a robust consent mechanism, ensuring data is accessed only with the explicit, granular, revocable, and traceable approval of the user.

In India, AAs serve as essential consent managers within the financial ecosystem, facilitating secure and transparent data sharing between individuals and financial institutions. This role is particularly important under DEPA and the DPDP Act, 2023, both of which emphasise individual control over personal data.

The DPDP Act introduces the Consent Manager framework as a regulatory mechanism to streamline and standardise the processing of personal data. In contrast, the RBI’s 2016 AA framework has operated for several years, focusing on the secure and consent-driven sharing of financial data. While both frameworks emphasise user consent, the DPDP Act and its Draft Rules apply these principles more broadly across sectors beyond finance.

Given the conceptual similarities between Consent Managers and the AA framework—and the fact that Reserve Bank Information Technology Private Limited (ReBIT) has already developed core technical specifications for Account Aggregators—it is likely that Consent Managers will be expected to adhere to comparable technical standards.

With the DPDP Act formally embedding personal data protection within a legal framework, businesses handling consumer data must now operate in a more structured, compliance-driven environment. Aligning the Consent Manager framework with the existing AA system will be crucial to preventing redundancy and creating a seamless, consent-based data-sharing ecosystem across both financial and personal domains. The long-term success of these initiatives will depend on rigorous enforcement, technological integration, and user education to ensure that individuals can actively manage and control their data.

DEPA and the DPDP Act could form a backbone for frameworks and regulations in India by addressing key aspects of data sharing, consent, and security.

- **Consent-driven Data Sharing:** DEPA's focus on consent management, particularly through AAs, directly supports the core principle of open banking—enabling secure and permissioned data sharing between financial institutions and third-party providers. The DPDP Act reinforces this by legally mandating consent for data processing, ensuring that open-banking transactions are grounded in user authorisation. Together, they offer a combined approach for accessing and using customer data within the open-banking ecosystem.
- **Empowering Customers:** Both frameworks empower customers with control over their financial data. DEPA enables individuals to grant granular access to their data through AAs, specifying what data can be shared and for what purpose. The DPDP Act complements this by granting data principals the rights to access, correct, and erase their data, reinforcing user control within the open-banking landscape. This user-centric approach fosters trust and encourages participation in open-banking initiatives.
- **Secure and Interoperable Infrastructure:** DEPA's integration with India Stack provides a robust and secure infrastructure for open banking. By leveraging existing digital infrastructure like Aadhaar and the Unified Payments Interface (UPI), it enables streamlined, interoperable data sharing across ecosystem players. The DPDP Act provides the legal framework that governs this data sharing, ensuring it happens within the boundaries of data protection principles. This combination is essential

for the seamless and secure flow of financial information that open banking requires.

- **Regulatory Clarity and Accountability:** The DPDP Act's establishment of a Data Protection Authority (DPA) provides a clear regulatory framework for open banking. The DPA will oversee data fiduciaries, including AAs and other financial institutions, ensuring compliance with data protection laws. This regulatory oversight is crucial for building trust and ensuring the responsible growth of open banking in India. DEPA's anticipated DPA (although the DPDP Act consolidates this) further reinforces this focus on accountability within the consent management process.
- **Data Security as a Priority:** Both DEPA and the DPDP Act prioritise data security, which is paramount for the success of open banking. DEPA establishes standards for secure data sharing through its consent-based architecture, while the DPDP Act mandates that data fiduciaries implement robust security measures to protect personal data. This focus on security builds confidence among users and mitigates the risks associated with data sharing in an open banking environment.

DEPA and the DPDP Act lay the foundation for a thriving open banking ecosystem in India. They establish a framework for consent-based data sharing, empower customers with control over their financial information, ensure secure and interoperable infrastructure, and provide regulatory clarity and accountability. By addressing these fundamental elements, these frameworks are fostering innovation and growth in India's financial sector.

# Enabling Open Banking: Account Aggregators as Consent Managers

The AA model<sup>11</sup> in India is a consent-driven data-sharing framework aimed at improving financial inclusion and streamlining access to financial services. It is a pillar of the open banking ecosystem, allowing individuals and businesses to securely share their financial data across banks, NBFCs, insurers, mutual funds, and other financial institutions while maintaining privacy safeguards. The system involves three entities: Financial Information Providers (FIPs), which hold the data; Financial Information Users (FIUs), such as lenders and wealth managers, who require the data to offer services; and AAs, licensed intermediaries that facilitate secure data transfer between FIPs and FIUs without storing or processing the data themselves. AAs operate based on explicit user consent, ensuring that data is shared only when authorised by the account holder. This framework enhances financial transparency, credit accessibility, and digital lending efficiency, facilitating financial transactions while prioritising data security and privacy.

AAs act as intermediaries, enabling individuals to share their financial data with service providers such as banks, insurance companies, and investment firms, based on explicit consent. This aligns with the DPDP Act's principles, which mandate that personal data can only be processed with the informed consent of the data principal (the individual whose data is being shared). AAs allow users to efficiently manage their consent, enabling them to decide what data to share, with whom, and for what purpose.

The AA ecosystem has seen remarkable growth, surpassing 140 million consents as of December 2024.<sup>12</sup> This rapid adoption indicates a growing comfort among users regarding consent management and data sharing. AAs facilitate access to financial services while building trust through secure and transparent data-sharing mechanisms. Operating independently of FIUs, AAs provide users with a centralised platform to manage consents without interference from data-requesting entities.

# Milestones and Achievements

**T**he AA framework has become a pivotal development in India's financial ecosystem, transforming the secure management and exchange of financial data. Introduced by the RBI on 2 September 2021, it has rapidly gained traction, marking milestones in a relatively short period of time.

## Rapid Growth and Adoption

As of December 2024, over 140 million consent requests have been successfully processed through AAs, with an estimated 7–8 percent of India's population already registered to manage and authorise the sharing of their financial data. The AA ecosystem continues to expand at a monthly cumulative consent request growth rate of approximately 13 percent.<sup>13</sup> This rapid expansion positions India as the fastest-growing open finance ecosystem globally, underscoring the increasing trust and acceptance of consent-driven data sharing.

## Expanding Use Cases

Originally conceptualised to optimise loan underwriting, the AA framework has expanded to encompass an array of financial services, including personal finance management, portfolio monitoring, fraud detection, and insurance policy issuance. By facilitating the secure, real-time exchange of authenticated financial data, AAs enable financial institutions to enhance decision-making, streamline customer onboarding, and improve the accuracy of credit assessments.

## Driving Financial Inclusion

AAs are playing a role in addressing financial inclusion challenges in India. With over 800 million individuals still lacking access to formal banking services, the AA framework provides a secure and efficient mechanism for facilitating financial data sharing between individuals, lenders, and service providers. By streamlining data accessibility and reducing traditional credit barriers, AAs enhance the ability of underserved populations to engage with the formal financial system.

# Milestones and Achievements

## **Collaboration with Financial Institutions**

The effectiveness of the AA framework is underpinned by a well-integrated ecosystem of financial institutions. As of August 2024, the framework encompasses 155 FIPs and 475 FIUs, including leading public banks.<sup>14</sup> This extensive adoption enables individuals to aggregate and access their financial data—including bank deposits, insurance policies, and mutual fund holdings—through a unified platform. The AA ecosystem has seen remarkable growth, surpassing 140 million consents as of December 2024.<sup>15</sup>

## **Future Prospects**

The penetration of AAs is expected to increase, as projections suggest that, by FY 2025, usage could reach 15-20 percent of the adult population, with potential growth to 25 percent by the end of 2025.<sup>16</sup> As awareness rises and technological advances are made, AAs are poised to play a more crucial role in India's digital economy, making financial transactions more efficient, transparent, and user-friendly.

# Addressing Challenges

India's AA system represents advancements in financial data accessibility, aiming to create a seamless, digital-first experience for consumers. However, despite its transformative potential, widespread adoption is impeded by various obstacles. Addressing these challenges is crucial to unlocking the full benefits of the AA framework and ensuring its role in fostering a more inclusive and efficient financial ecosystem.

## Fixing Gaps

A joint account holder can share financial information with an FIU via an AA, but the process requires consent from all joint account holders. This prevents users from benefiting from a seamless, digital financial ecosystem. Due to the often complex nature of financial information, users may struggle to fully comprehend the scope of the consent they are granting. This lack of clarity can result in unintended data access by FIUs, potentially leading to overreach and exposing users to risks such as data-driven profiling and targeted advertising.

## Increasing Participation

Although most big banks have integrated with the AA system, a number of prominent institutions have yet to join the network.<sup>17</sup> This includes small finance banks like Equitas Bank, private-sector banks like Bandhan Bank and DCB Bank, and foreign banks like Bank of America and Deutsche Bank.<sup>18</sup> This partial adoption has led to a fragmented financial landscape, limiting the system's widespread implementation. The absence of these banks restricts access for a population of users, preventing them from fully utilising the benefits of the AA framework. This lack of universal participation hinders the broader objective of establishing a seamless, paperless financial ecosystem, where individuals can access their financial data irrespective of their banking provider.

## Standardisation

A challenge hindering widespread adoption of the AA system is the inconsistency in data quality. Many banks have yet to implement standardised data practices, leading to inefficiencies and confusion for end users.<sup>19</sup> A prominent issue is the variation in transaction timestamps, with different

# Addressing Challenges

banks employing inconsistent formatting, resulting in discrepancies that can mislead users. Although these inconsistencies may seem minor, they can impact individuals who rely on precise financial data for effective financial management. Similarly, inconsistencies in transaction dates have led to errors such as missed loan repayments and financial miscalculations. The lack of uniform transaction descriptions further exacerbates the problem, making it difficult for users to clearly interpret their financial activity.

## Improving Performance

While some banks have made progress in integrating with the AA system, many public sector banks continue to face performance challenges. These institutions often struggle to scale their infrastructure to accommodate the volume of data requests required by the AA framework, leading to inconsistent and unreliable data access. Notably, being listed as “live” on the Sahamati platform does not guarantee real-time data availability from an FIP. Sahamati<sup>20</sup> (Sahamati Foundation) is a member-led industry alliance established to support and advance the Account Aggregator ecosystem in India. It operates as a not-for-profit private limited company under Section 8 of the Companies Act, 2013. Users frequently encounter difficulties with account discovery and data retrieval, experiencing persistent issues. These operational bottlenecks undermine the reliability of the AA system, causing frustration for users who rely on seamless and efficient financial data sharing.

# A Global Perspective on Open Banking

India's open banking ecosystem is expanding. While challenges persist, many are likely to be addressed as the system matures. At the same time, examining other open banking frameworks is essential—not only to assess India's progress but also to extract insights and anticipate potential obstacles. The United Kingdom (UK) and Australia, with more advanced open banking ecosystems, offer valuable points of comparison. However, their approaches differ from India's, shaped by distinct regulatory environments, economic priorities, and consumer needs. These variations provide a unique opportunity to analyse how country-specific frameworks evolve under the broader momentum of open banking.

## Regulatory Approaches: UK and Australia

The UK's open banking framework was established in 2017 through the Competition and Markets Authority's (CMA)<sup>21</sup> Open Banking to address competition concerns in retail banking. The order required the nine largest banks (CMA9)<sup>22</sup> to develop secure, standardised APIs, enabling licensed third-party providers (TPPs) to access customer financial data with explicit consent. The aim was to enhance transparency, consumer choice, and financial innovation. Mandates included API standardisation, phased implementation, and strong consumer protection measures such as Strong Customer Authentication (SCA). To oversee this transition, the CMA created the Open Banking Implementation Entity (OBIE) in 2016 to develop technical standards, ensure compliance, promote adoption, and safeguard consumer data. Over time, open banking in the UK has evolved beyond payments and account data into broader financial services, setting the foundation for open finance.

In 2022, regulatory oversight began transitioning from the OBIE to the Joint Regulatory Oversight Committee,<sup>23</sup> co-led by the Financial Conduct Authority (FCA) and the Payment Systems Regulator (PSR), to ensure long-term sustainability and expansion. The UK's open banking framework has since become a global benchmark, fostering competition, financial inclusion, and technological innovation.

The Consumer Data Right (CDR) governs Australia's open banking framework,<sup>24</sup> introduced in 2019 to give consumers greater control over their financial data. Unlike traditional open banking models, the CDR spans multiple sectors—including energy and telecommunications—making it a

# A Global Perspective on Open Banking

broader data-sharing initiative. The Australian Competition and Consumer Commission (ACCC)<sup>25</sup> formed in 1995 oversees compliance, while the Office of the Australian Information Commissioner (OAIC) of 2010<sup>26</sup> enforces privacy and data protection regulations.

Australia's open banking was rolled out in phases, with the four biggest banks—Commonwealth Bank, Westpac, Australia and New Zealand Banking (ANZ), and National Australia Bank (NAB)—required to comply by 2020, followed by smaller financial institutions. The regulations require banks to provide consumers and accredited third parties secure access to financial data, promoting competition and innovation in financial services. Unlike the UK's open banking, which is driven by competition mandates, Australia's model emphasises consumer empowerment, allowing users to share their data across service providers to access better financial products.

# Mandated vs. Market-Driven

The AA model is advancing, making it essential to examine alternative frameworks for a comprehensive understanding of open banking. Analysing these models highlights the motivations behind open banking adoption in different countries. Comparative assessments offer valuable insights, uncovering opportunities to refine and enhance the AA ecosystem.

## A Mandated, Top-Down Approach

The UK's open banking framework was developed following the Competition and Markets Authority's (CMA) 2016<sup>27</sup> investigation into the retail banking sector. This regulatory intervention required the nine largest banks, collectively referred to as the CMA9, to implement open banking by developing standardised APIs. These APIs enable TPPs to securely access consumer financial data, promoting competition and innovation in the financial sector. To oversee implementation and ensure compliance, the OBIE was established, tasked with facilitating interoperability and adherence to regulatory standards.

The UK's open banking model is primarily compliance-driven, incorporating robust consumer protection mechanisms under the Payment Services Directive 2 (PSD2).<sup>28</sup> A key requirement of this directive is the enforcement of strong customer authentication (SCA) and consent-based data-sharing practices, ensuring secure and user-controlled access to financial data.

Australia's open banking framework, introduced as part of the broader Consumer Data Right (CDR) legislation in 2019, extends beyond financial services to other sectors including energy and telecommunications. The CDR's initial phase focused on open banking, mandating banks to securely share consumer financial data with accredited third parties to enhance competition and improve consumer choice.

The Australian Competition and Consumer Commission (ACCC) and the Office of the Australian Information Commissioner (OAIC) jointly manage the regulatory oversight of Australia's open banking framework. These regulatory bodies ensure compliance with rigorous data security and privacy standards. While major banks were required to comply by 2021, smaller financial institutions have been granted a phased implementation timeline to facilitate a smoother transition.

# Mandated vs. Market-Driven

## India: A Market-Led, Consent-Driven Model

India's approach to open banking is market-driven, facilitated by the foundational digital infrastructure known as India Stack. This ecosystem comprises key components such as Aadhaar, the UPI, and the AA framework. Unlike regulatory-driven models observed in jurisdictions such as the UK, India's open banking framework has evolved through voluntary participation by banks and financial institutions, guided by the RBI and its subsidiary, the Reserve Bank Information Technology Pvt Ltd (ReBIT) founded in 2016.<sup>29</sup>

A key distinction in India's open banking model is its reliance on the DEPA, which provides a consent-based mechanism for data sharing. This framework ensures that individuals retain control over their financial information, granting explicit consent for data access through AAs. By prioritising user empowerment and secure data exchange, DEPA aligns with India's broader objectives of fostering financial inclusion while maintaining stringent data protection standards.

The adoption of the UK's open banking framework has been slower than anticipated, despite regulatory mandates designed to facilitate its implementation. As of 2024, only approximately 11 percent<sup>30</sup> of UK consumers actively engage with open banking services, reflecting a gap between policy intentions and user adoption. However, the framework has played an important role in fostering fintech innovation, with over six million users utilising open banking-enabled applications for financial management, lending, and account aggregation. One of the primary barriers to broader adoption has been the delayed implementation of high-quality APIs by banks, hindering both innovation and service expansion. Regulatory complexities and consumer hesitancy have also contributed to the slower uptake.

India's AA framework has demonstrated higher adoption rates, with over 100 million consent-based data-sharing requests processed by 2024<sup>31</sup> and an estimated 80–90 million users on-boarded.<sup>32</sup> The adoption trajectory of the AA ecosystem closely mirrors that of the UPI, positioning India among the fastest-growing open finance markets globally. Unlike the UK's model, which remains largely restricted to banking services, India's approach extends across multiple financial sectors, including wealth management, insurance, and lending. This broader scope, combined with India's well-established digital infrastructure—comprising UPI, the DEPA, and India Stack—has facilitated

# Mandated vs. Market-Driven

rapid integration. Furthermore, India's emphasis on financial inclusion has driven substantial real-world impact, whereas the UK's competition-oriented model has faced challenges in achieving mainstream consumer adoption.


**Table 1: Open Banking Models: UK, Australia, and India**

	UK	Australia	India
<b>Approach</b>	Regulatory-driven (CMA & PSD2)	Regulatory-driven (CDR mandate)	Market-led, consent-driven (AA Framework)
<b>Regulatory Body</b>	OBIE, FCA, CMA	ACCC, OAIC, Data Standards Body	RBI, ReBIT, Sahamati
<b>Implementation</b>	Top-down enforcement by CMA	Top-down enforcement	Bottom-up participation by banks and NBFCs
<b>Scope of Data</b>	Primarily payments and banking data	Broader (includes energy & telecom)	Wider scope, potentially insurance, mutual funds, pensions
<b>Adoption Pace</b>	Slower due to regulatory compliance burden	Slower due to compliance complexity	Faster due to voluntary fintech adoption
<b>Focus</b>	Competition & innovation in banking	Consumer rights & competition	Financial inclusion & data empowerment

India's open banking ecosystem may be nascent but is growing rapidly. While challenges persist, they are anticipated to be resolved over time. Looking ahead, enhancing the AA system and expanding its applicability across financial services will be essential.

To fully realise the potential of open banking, India must focus on expanding interoperability, enhancing data integration, and facilitating cross-border financial access. Standardised data-sharing templates are particularly important for enabling seamless cross-border financial transactions. In the long term, open finance should support global financial integration by fostering interoperability across open banking frameworks. Given the importance of trade finance, a coordinated global approach to open banking can help businesses and financial institutions streamline transactions across borders.

India's open banking journey stands apart from the regulatory-driven models of the UK and Australia by prioritising financial inclusion. While the UK and Australia focus on competition and consumer protection, India leverages its existing digital infrastructure—including UPI, DEPA, and the AA framework—to drive rapid adoption. This market-driven strategy has allowed open banking to scale at an unprecedented pace, demonstrating that innovation flourishes when aligned with user needs and technological readiness.

As India's open banking ecosystem matures, it may eventually shift towards a competition-driven framework, similar to the UK and Australia. However, by achieving financial inclusion, India is laying a stronger foundation for long-term adoption of open finance. The experiences of Western economies, which have grappled with these issues for decades, offer valuable lessons in balancing security, innovation, and adoption. By learning from these models and adapting them to its own unique context, India has the potential to emerge as a global leader in open banking and demonstrate how financial technology can drive both economic growth and inclusion. 

**Sauradeep Bag** is Associate Fellow, Centre for Digital Societies, Observer Research Foundation.

- 1 Nydia Remolina, “Open Banking: Regulatory Challenges for a New Form of Financial Intermediation in a Data-Driven World,” Singapore Management University Centre for AI & Data Governance Research Paper No. 2019/05, October 2019, <https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=1006&context=caidg>.
- 2 Ministry of Electronics and Information Technology, Government of India, *The Digital Personal Data Protection Act, 2023*, (New Delhi: MEITY, 2023), <https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf>.
- 3 Planning Commission, Government of India, <https://pib.gov.in/newsite/PrintRelease.aspx?relid=88503>.
- 4 “ELP Discussion Paper on Justice B.N. Srikrishna Committee on Data Protection,” Economic Laws Practice (ELP), 2023, <https://elplaw.in/wp-content/uploads/2023/09/ELP-Discussion-Paper-Justice-BN-Srikrishna-Committee-Data-Protection-2.pdf>.
- 5 Ministry of Electronics and Information Technology, Government of India, *The Information Technology Act, 2000*, (New Delhi: MEITY, 2000), [https://www.indiacode.nic.in/bitstream/123456789/13116/1/it\\_act\\_2000\\_updated.pdf](https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf).
- 6 Justice K.S. Puttaswamy (Retd.) & Ors. vs. Union of India & Ors., <https://privacylibrary.ccgnlud.org/case/justice-ks-puttaswamy-ors-vs-union-of-india-ors#:~:text=The%20Bench%20unanimously%20held%20that,the%20Supreme%20Court%20in%20M.P>.
- 7 GDPR.eu, “What Is GDPR?,” <https://gdpr.eu/what-is-gdpr/>.
- 8 OECD, *Going Digital: Shaping Policies, Improving Lives*, Paris, 2020, OECD Publishing, <https://doi.org/10.1787/9789264311992-en>
- 9 Niti Aayog, *Data Empowerment and Protection Architecture: A Secure, Consent-Based Framework*, August 2020, <https://www.niti.gov.in/sites/default/files/2023-03/Data-Empowerment-and-Protection-Architecture-A-Secure-Consent-Based.pdf>.
- 10 Reserve Bank of India, *Master Direction - Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions*, 2016, [https://www.rbi.org.in/Scripts/BS\\_ViewMasDirections.aspx?id=10598](https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10598)
- 11 Sahamati, “What Is Account Aggregator,” <https://sahamati.org.in/what-is-account-aggregator/>.
- 12 Sahamati, “Reconciling the Account Aggregator and Consent Manager Frameworks,” March 18, 2025, <https://sahamati.org.in/reconciling-the-account-aggregator-and-consent-manager-frameworks/>
- 13 Sahamati, “Reconciling the Account Aggregator and Consent Manager Frameworks”
- 14 Sahamati, “FIP & FIU in Account Aggregators Ecosystem,” <https://sahamati.org.in/fip-fiu-in-account-aggregators-ecosystem/>.

- 15 Sahamati, “Reconciling the Account Aggregator and Consent Manager Frameworks”
- 16 Sahamati, “India’s Account Aggregator Framework Crosses 100 Million Consents in Three Years,” <https://sahamati.org.in/media-article/indias-account-aggregator-framework-crosses-100-million-consents-in-three-years/>.
- 17 Sahamati, “FIP & FIU in Account Aggregators Ecosystem”
- 18 Sahamati, “FIP & FIU in Account Aggregators Ecosystem”
- 19 Neil Borate, “Account Aggregator Fintech Startup Fold Money to Offer Bank Savings, Fixed Deposits, Credit, Loans, Mutual Funds,” *LiveMint*, February 20, 2024, <https://www.livemint.com/money/account-aggregator-fintech-startup-fold-money-bank-savings-fixed-deposit-credit-loans-mutual-funds-rbi-11732084804979.html>.
- 20 Sahamati, “Mission,” <https://sahamati.org.in/mission/>
- 21 Competition and Markets Authority, *Banking Providers Roadmap Completion Decision*, UK Government, 2017, [https://assets.publishing.service.gov.uk/media/63bed8958fa8f513b40f866c/BANKING\\_PROVIDERS\\_Roadmap\\_Completion\\_Decision\\_.pdf](https://assets.publishing.service.gov.uk/media/63bed8958fa8f513b40f866c/BANKING_PROVIDERS_Roadmap_Completion_Decision_.pdf).
- 22 Open Banking, “CMA9,” Open Banking Implementation Entity, <https://www.openbanking.org.uk/glossary/cma-9/>.
- 23 Financial Conduct Authority, “Future of Open Banking and the Joint Regulatory Oversight Committee,” June 21, 2022, <https://www.fca.org.uk/firms/future-open-banking-joint-regulatory-oversight-committee>.
- 24 Consumer Data Right, Australian Government, <https://www.cdr.gov.au/>.
- 25 Australian Competition & Consumer Commission, Commonwealth of Australia, <https://www.accc.gov.au/>.
- 26 Office of the Australian Information Commissioner, Australian Government, <https://www.oaic.gov.au/>.
- 27 Open Banking , “Regulatory,” Open Banking Implementation Entity, <https://www.openbanking.org.uk/regulatory/>.
- 28 European Central Bank , *The Revised Payment Services Directive (PSD2) and What It Means for You*, March 2018, [https://www.ecb.europa.eu/press/intro/mip-online/2018/html/1803\\_revisedpsd.en.html](https://www.ecb.europa.eu/press/intro/mip-online/2018/html/1803_revisedpsd.en.html).
- 29 Reserve Bank Information Technology Pvt Ltd, “Home,” <https://rebit.org.in/>.
- 30 Open Banking, *Open Banking Impact Report – October 2023*, Open Banking Limited, 2023, <https://www.openbanking.org.uk/news/open-banking-impact-report-october-2023/>.
- 31 Sahamati, “India’s Account Aggregator Framework Crosses 100 Million Consents in Three Years,”
- 32 Sahamati, “India’s Account Aggregator Framework Crosses 100 Million Consents in Three Years”



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](mailto:contactus@orfonline.org)  
Website: [www.orfonline.org](http://www.orfonline.org)