Governance, Openness and Security of Digital Public Infrastructure in India

internet Research Lab

March 2026

1 Introduction

Digital Public Infrastructure (DPI) is quickly becoming a cornerstone of government policy. Governments, development agencies, and multilateral institutions increasingly promote DPI as a framework for expanding public service delivery, fostering digital economies, and enabling large-scale systems of identification, payments, and data exchange. [1] In policy discourse, DPI is often framed as a foundational layer of digital development that can improve efficiency, expand inclusion, and support innovation across both public and private sectors. As a result, the concept has gained significant traction in global development agendas and international policy forums.

Despite its growing prominence, however, DPI remains a concept that is both under-defined and politically loaded. Much of the effort to define DPI has emerged only after the implementation of large-scale digital systems that are now retrospectively categorized under the DPI label. These post-hoc conceptualizations are often tied to efforts to replicate perceived "success stories" in other countries, particularly through development cooperation and technology transfer initiatives. As a result, many of the infrastructures labeled as DPI were not originally designed with a coherent DPI framework in mind, and do not necessarily embody the values – such as openness, inclusivity, security, and accountability – that are commonly associated with the model in policy discourse.

This paper examines the gap between the normative promises of DPI and the operational characteristics of existing DPI systems. Specifically, we analyze six digital infrastructures implemented in India and evaluate them against a set of attributes commonly presented as defining features of the DPI approach. These attributes are drawn largely from policy frameworks and narratives advanced by the Indian state and associated international institutions. By examining how these systems function in practice – including their governance structures, economic models, data practices, and openness – we aim to assess whether they meaningfully reflect the principles that DPIs are said to typify.

India provides a particularly important context for this research: it has developed some of the most widely cited DPI systems, and has actively promoted its model in international forums and development partnerships. [2] Yet, many of claims surrounding the properties of DPI remain insufficiently examined in relation to the actual functioning of India's digital systems. As one of the earliest and most expansive adopters of DPI, India serves as a useful case study to interrogate both the promises and limitations of this evolving governance model.

The rest of the paper paper is structured as follows. First, we summarise how DPI has been conceptualized across academic, policy, and institutional sources, with particular attention to the features and values commonly associated with the DPI model. We move on to discuss the formulation, development and deployment of DPIs in India. Then, we summarise our evaluation framework and methodology with respect to individual features and values commonly associated with the DPI model, including public ownership, governance, openness, security and privacy. Using this framework, we analyse six DPI systems in India:

- *FASTag* – electronic toll collection system
- *Aadhaar eKYC* – biometric identity verification
- *DigiLocker* – digital document storage platform

[DRAFT — compiled at 2026-05-08 7:27; not for distribution]

- *Account Aggregator* – financial data sharing
- *Bharat Connect* – unified bill payment system
- *Unified Payments Interface* – digital payments system

Finally, we examine how this evaluation of design and operation of DPIs in India aligns with, or diverges from, the characteristics commonly associated with DPI.

2 Digital Public Infrastructure: Concept and Indian Practice

Digital public infrastructure (DPI) refers, at its broadest, to shared digital systems that underpin participation in society and markets. The term itself has a short intellectual history, and no authoritative definition commands universal agreement. Its genealogy can be traced through three phases: a dispersed, ad hoc period of usage roughly from 2012 to 2020; a phase of consolidation around an Indian-influenced model between 2020 and 2024; and an ongoing phase of localization and critical scrutiny as the concept is adopted and adapted globally [3].

The earliest uses of the term were uncoordinated, appearing in discussions about open data, deliberative democracy, and digital commons without any shared conceptual framework [3]. Zuckerman proposed DPI as intentionally designed digital social spaces—publicly funded alternatives to surveillance-capitalist platforms, structured around civic rather than commercial values [4]. Building on Frischmann's conception of infrastructure as "shared means to many ends," Zuckerman argued that just as governments invest in roads or public broadcasting, they should invest in digital spaces designed to enable citizenship [4]. This vision of DPI as communicative infrastructure coexisted with, but remained largely disconnected from, the logistical tradition that would come to dominate global policy [5].

The consolidating model was shaped decisively by the Indian experience. India's DPI trajectory began in the early 2010s, driven by a concrete administrative problem: pervasive leakage in welfare benefit delivery to a vast and dispersed population. Aadhaar, a biometric identity system launched by the Unique Identification Authority of India under Nandan Nilekani, was designed to provide a reliable identity layer that would eliminate fraudulent or duplicate beneficiaries and enable direct benefit transfers [6]. The architects conceived this identity layer not as a terminal product but as a foundation: a shared digital good on which successive systems could be layered. UPI (interoperable real-time payments), DigiLocker (authenticated digital document access), and DEPA (consent-based data sharing) each built on the identity layer and on one another, composing what became known as the India Stack: a modular, layered architecture intended to support both state service delivery and private sector innovation [6, 7].

Since 2020, a transnational coalition of funders, multilateral institutions, and policymakers actively promoted this model globally [3]. The Centre for Digital Public Infrastructure has articulated five architectural principles that distinguish DPI from conventional digitisation: interoperability; minimalist and reusable building blocks; diverse and inclusive innovation ecosystems; federated and decentralised design; and security and privacy by design [8]. Eaves and Sandman offer a function-oriented complement: DPI as society-wide digital capabilities essential for participation in markets and civic life, which public institutions must guarantee to be inclusive, foundational, interoperable, and publicly accountable [7].

This model received formal multilateral endorsement at the G20 under India's 2023 presidency, which defined DPI as a set of shared digital systems, built on open standards and specifications to deliver equitable access to public and private services at societal scale, governed by legal frameworks designed to promote development, inclusion, innovation, trust, and competition [9]. The same document acknowledged DPI to be an "evolving concept" adaptable to country contexts, reflecting real definitional instability [9]. International bodies have also diverged in their emphases: the G7's 2024 Ministerial Declaration framed DPI primarily as an enabler of state-led digital public services, while the OECD positioned it as a category of government digital infrastructure for delivering access to both public and private services.[10, 11]. Eaves and Rao, drawing on grounded theory methodology and expert interviews, identify normative attributes common across frameworks such as interoperability, transparency and accountability, privacy and safety protection, and inclusion [12].

Critics have challenged both the model and the discourse. Samdub argues the vagueness of DPI is itself a political strategy, allowing states and firms to cloak choices about ownership and control in the neutral

[DRAFT — compiled at 2026-05-08 7:27; not for distribution]

language of digital commons [3]. IT for Change contend that India's own DPI architecture has generated a techno-patrimonial regime in which private actors capture data dividends, welfare delivery resembles a data marketplace, and public value creation is undermined [13]. These tensions are not peripheral to the DPI debate but constitutive of it, and they structure the analysis that follows.

India is the site of the world's most advanced and extensively studied DPI ecosystem, and it is the focus of this paper. We examine a representative subset of Indian DPIs that span identity, payments, documents, health, commerce, and mobility. Each is treated as a discrete DPI, though they share infrastructure, governance actors, and data-linking mechanisms.

- **Aadhaar**: Biometric identity system issuing unique identifiers to residents, used as the foundational identity layer across the Indian DPI stack.
- **FASTag**: Radio-frequency identification system enabling electronic toll collection (Section 4.1).
- **Aadhaar e-KYC**: Digital identity verification service allowing authorised entities to authenticate individuals via Aadhaar (Section 4.2).
- **DigiLocker**: Platform for issuing, storing, and verifying digital credentials (Section 4.3).
- **DigiYatra**: Facial recognition-based system enabling paperless boarding at Indian airports by linking biometrics to a traveller's identity credentials.
- **Account Aggregator**: Financial data-sharing framework allowing individuals to share verified financial information across institutions (Section 4.4).
- **Bharat Connect**: Bill payment platform enabling consumers to pay utility, tax, and subscription bills (Section 4.5).
- **Open Network for Digital Commerce**: Network enabling interoperable buyer-seller transactions across platforms.
- **Unified Payments Interface (UPI)**: Real-time payment system enabling fund transfers across bank accounts via mobile devices (Section 4.6).
- **eSign**: Digital signature service that uses Aadhaar-based authentication to enable electronic signing.

3 Evaluation framework and methodology

Despite the vagueness of the definition of the term *digital public infrastructure*, there is an emerging cohesion around what *principles* should motivate and inform the design of DPI. For instance, the Centre for Digital Public Infrastructure (CDPI) identifies "interoperability" and "reusable building blocks" as central to DPIs [8] – principles also espoused by the India Stack and Government of India in their publications in similar, if not the same, words. In the same vein, security and privacy of DPIs are explicitly called out by the G20 Digital Economy Ministers' Meeting Outcome Document and the CDPI. [9].

Note that this does not mean there is a consensus across the Government of India (or other governments), international organisations, academia and civil society around the contours of the principles or how they should be operationalised. In many cases, it is also unclear whether these principles or properties are meant to be descriptive or prescriptive.

In the following subsections, we summarise some of these properties and principles commonly understood as undergirding the development of DPI. Note that some of these properties are, of course, interrelated. For example, security generally benefits from a policy of openness around code. Similarly, openness advances accountability in governance, and is often a prerequisite to public participation in the technical aspects of DPIs.

We created an evaluation framework for DPIs using these principles, in an effort to empirically validate to what extent – if at all – DPIs in India live up to these aspirations and commitments. Our evaluation framework is detailed in Appendix A.

[DRAFT — compiled at 2026-05-08 7:27; not for distribution]

To select which DPIs in India to analyse, we restricted ourselves to projects explicitly described as DPI by the Union Government of India, and aimed to cover the most common applications and functionalities of DPI. Thus, in Section 4.1, we use the evaluation framework to analyse FASTag, Aadhaar eKYC, DigiLocker, Account Aggregator, Bharat Connect and Unified Payments Interface.

3.1 Introduction and ownership

Digital Public Infrastructures (DPIs) differ in how ownership and operation are structured, typically falling into three models: private, government-led, and hybrid or public-private partnerships (PPPs). [14] In private models, industry actors develop and run the infrastructure under public regulation. Current examples include Kenya's M-Pesa or Visa. Government-led models place the state in charge of design, operation, and rulemaking, as seen in India's Aadhaar or Brazil's Pix. [15] Hybrid models blend these approaches, with governments defining standards while private or semi-private entities build and operate the system, such as UPI in India or PromptPay in Thailand. [16]

For these aspects, we examine the ownership structure of the DPIs in question, and any larger consequences that arise from it. Although there is no prescriptive model for DPIs (they tend to be modelled around considerations such as availability of capacity and investment), the DPI approach emphasizes key attributes that align it with a broader participatory ecosystem. For example, Eaves and Rao consider successful systems to be those usually championed by a central authority that ensures coherence across agencies, while maintaining a balance between public regulation (trust frameworks, interoperability standards) and private participation (innovation, scalability, financial sustainability). [12]

3.2 Development and deployment

This section examines how each DPI system was conceived, designed, and implemented, and which actors were involved in this process. It considers whether the infrastructure was developed solely by government agencies, delegated to private actors, or created through collaborative or participatory processes involving multiple stakeholders. Where relevant, it also looks at whether there were opportunities for public consultation, co-creation, or input from civil society and affected users during the design and rollout of the system.

Notably, it identifies the actors responsible for the ongoing development and operation of the infrastructure, including government bodies, private companies, financial institutions, and technology providers. Understanding these roles helps clarify how responsibility is distributed across the ecosystem and whether the system is operated as a centralized public service or through a decentralized network of intermediaries.

3.3 Governance

Governance structures determine how DPI systems are controlled, regulated and made accountable. This includes identifying who governs the system, what powers they exercise, and the tools used to enforce these powers, such as legislation, regulatory frameworks, contracts, and technical standards. Governance may be exercised directly by government agencies, delegated to independent authorities, or shared across public and private actors.

Especially relevant to this analysis is the extent and nature of state involvement. In some DPIs, governments act as direct operators, setting and enforcing rules while also managing day-to-day operations. In others, the state plays a more limited role, focusing on regulatory oversight while delegating implementation and operation to private or hybrid entities. [14] Increasingly, DPI ecosystems rely on models of co-regulation, where governance functions are distributed across regulators, infrastructure operators, and private intermediaries. [14] These arrangements often involve certification processes, audit requirements, compliance monitoring, and the ability to suspend or terminate access for non-compliant actors.

Governance structures also determine who can participate in the ecosystem and under what conditions. Entry barriers may include regulatory licensing requirements, technical certification, financial thresholds, or contractual approval processes. While such controls may be justified on grounds of security, interoperability, or system integrity, they also shape market dynamics and influence which actors are able to build services on top of the infrastructure. Examining governance therefore provides insight into how authority is exercised

[DRAFT — compiled at 2026-05-08 7:27; not for distribution]

within the system, how accountability is maintained, and whether the infrastructure functions as an open public utility or a tightly controlled institutional network.

3.4 Economic and business models

DPI systems operate under a range of economic and business models, reflecting differences in ownership, governance, and intended public function. Some DPIs are fully funded and operated by governments as public goods, with costs borne through public expenditure and no direct charges to users. Others adopt hybrid models, charging fees to participating institutions such as banks, service providers, or integrators, while maintaining free or subsidized access for end users. Still others incorporate explicitly commercial components, allowing private intermediaries to generate revenue through transaction fees, value-added services, or data-driven products built on top of the infrastructure. [17]

These economic structures shape how DPIs evolve and whose interests they ultimately serve. Profit-oriented models can incentivize rapid innovation, expansion, and private sector participation, but may also create tensions between commercial objectives and public interest goals such as privacy, equity, and universal access. Conversely, systems that rely entirely on government funding may prioritize public service delivery and inclusion, but can face sustainability challenges if political priorities or fiscal allocations change. Hybrid models – combining public funding, regulated participation fees, and private sector involvement – attempt to balance these considerations, but often introduce complex incentive structures across multiple actors.

Understanding the economic and business model of a DPI is therefore critical to assessing its long-term sustainability, accessibility, and governance. It reveals not only how the infrastructure is financed, but also which actors benefit from its operation, how costs and risks are distributed, and whether the system functions primarily as a public utility, a regulated market platform, or a commercial ecosystem built on publicly established rails

3.5 Openness

Openness is widely considered a defining characteristic of DPI, but its meaning and implementation vary significantly across systems. Openness can exist at multiple levels, including open-source software, open standards, open APIs, and open participation models. [14] Each of these dimensions has distinct implications for how infrastructure functions and evolves. For instance, open-source code can enable independent auditing, transparency, and reuse, while open standards can promote interoperability across providers without requiring full public access to underlying code. [14] At the same time, decisions around openness are often shaped by trade-offs involving security, institutional capacity, cost, and the degree of control that governments or operators seek to retain. [12]

International frameworks such as the United Nations' open-source principles emphasize that openness should go beyond technical access to include broader ecosystem participation. These principles promote approaches such as "open by default," encouraging reuse and interoperability, enabling community participation, providing clear documentation, and ensuring that systems can be sustained and scaled over time. [18] In practice, however, many DPI systems adopt selective openness – allowing controlled access to technical standards or APIs while restricting direct access to source code or governance processes.

In this study, openness is evaluated through several indicators, including whether source code or technical components are publicly available, whether APIs are openly accessible or restricted to authorized participants, whether development occurs transparently, and whether external actors can contribute to or influence the system's evolution. Additional factors include the existence of open-source communities, contribution policies, public documentation, and transparency mechanisms such as operational status reporting. Examining these factors helps assess whether a DPI functions as a truly open public resource or as a permissioned infrastructure with limited transparency and participation.

3.6 Coercion

The adoption of DPI is often presented as a measure of its success, reflecting its reach, usability, and integration into everyday life. However, adoption does not always occur through voluntary uptake alone. [19] In many cases, elements of coercion, either direct or indirect, play a significant role in driving participation.

[DRAFT — compiled at 2026-05-08 7:27; not for distribution]

Direct coercion may take the form of legal mandates requiring individuals, businesses, or public institutions to use the infrastructure. Indirect coercion may arise when access to essential services, benefits, or markets becomes contingent on using the system, or when alternative mechanisms are gradually phased out, made less convenient, or rendered unavailable.

These dynamics have important implications not only for user autonomy but also for market competition and the broader digital ecosystem. When the state actively promotes or mandates a particular infrastructure, it can create structural advantages over private alternatives, shaping market outcomes and limiting meaningful choice. Examining coercion therefore helps distinguish between organic adoption and adoption driven by regulatory or structural pressures, and provides insight into how state power, public service delivery, and market competition interact within DPI ecosystems.

3.7 Data collection practices

DPI systems rely fundamentally on the collection, processing, and exchange of data to function effectively. These systems are often designed to facilitate seamless transactions, enable interoperability across services, and support data-driven decision-making by governments and service providers. [14] Relatedly, the collection and use of data forms a crucial profit incentive for players in the system. [20] As a result, the type, volume, and quality of data collected and/or created form a core component of the DPI model. This includes data provided during registration, data generated through transactions and interactions, and metadata created as part of system operations.

This section examines the full lifecycle of data within each DPI system. It considers what data is collected directly from users, what data is obtained from or linked to other databases, and what new data is created through usage. It also looks at where this data is stored, how long it is retained, which actors have access to it, and under what conditions it may be shared or disclosed. Governance mechanisms – including legal frameworks, technical safeguards, and institutional controls – play an important role in shaping these practices.

Data practices in DPI systems often involve trade-offs between efficiency, interoperability, and privacy. [17] While data sharing and integration can improve service delivery and enable innovation, they can also expand the scope of surveillance, increase the number of actors with access to sensitive information, and create risks related to misuse or breaches. Understanding how data is collected, stored, linked, and governed is therefore essential to evaluating the broader policy implications of DPI systems and their impact on individual rights and institutional accountability.

3.8 Data sharing and linking with other databases

Interoperability is often presented as a core design feature of digital public infrastructure. This capacity for interoperability frequently depends on structured data exchange frameworks, shared technical standards, and the use of common identifiers that allow records to be matched across systems. [12]

Data sharing within DPI ecosystems may occur in multiple ways. It can involve direct exchanges between participating entities as part of a transaction, integration with other government or private databases, or the use of identifiers allocated by external systems (such as the Aadhaar number, a bank account number, or a mobile phone number) to authenticate or retrieve information. In many cases, these linkages are framed as consent-based, meaning that user authorization is formally required before data is transmitted. However, the design of consent flows, the clarity of disclosures, and the structural dependence on linked identifiers can significantly shape how meaningful that consent is in practice.

This section examines how each DPI enables data sharing and interoperability, including the technical and legal mechanisms that govern linkages with other systems. It considers which identifiers are used to connect datasets, how information flows between actors, and whether limits exist on onward sharing or secondary uses. Because interoperability enhances efficiency and scalability, it is often central to the DPI model – but it also expands the network of entities that can access user data. These features are therefore critical to assessing both the benefits and privacy implications of the DPI design.

[DRAFT — compiled at 2026-05-08 7:27; not for distribution]

3.9 Data security and privacy

In the preceding sections, we examine what data DPI systems collect, share, and link. We now address how that data is protected and what obligations arise when those protections fail. For infrastructure operating at population scale, the consequences of a security failure are correspondingly severe: a breach affecting a central payment processor or identity repository may simultaneously expose the sensitive data of hundreds of millions of individuals.

We evaluate security practices through public disclosure, institutional process, and regulatory compliance. The first indicator is whether the system operator makes affirmative public statements about its security posture: certifications held, architectural commitments such as zero-trust design, and the existence of continuous monitoring capabilities. The second is the accessibility of vulnerability disclosure processes: whether a defined channel exists for reporting security flaws, whether bug bounties are offered, and whether discovered vulnerabilities are disclosed to users or to the Indian Computer Emergency Response Team (CERT-IN). Under Indian law, all ICT system operators are subject to a mandatory six-hour incident-reporting requirement for data breaches affecting payment systems. Compliance with this requirement, and the extent of any corresponding disclosure to affected users, is examined for each system.

We further consider breach disclosure obligations in light of the Digital Personal Data Protection Act, 2023, which will require notification to both the Data Protection Board and affected individuals following unauthorised processing or accidental data loss. We note the gap between current practice and this forthcoming standard where relevant.

Together, these indicators distinguish systems that treat security as a performative compliance exercise from those that embed it as a substantive operational commitment.

4 Findings

4.1 FASTag

4.1.1 Introduction and ownership

The FASTag system, developed under India's National Electronic Toll Collection (NETC) program, is designed to enable toll payments using Radio Frequency Identification (RFID) tags affixed to vehicles. [21] Each transaction is automatically debited from the user's linked account as the vehicle passes through a toll plaza. The NETC ecosystem is interoperable and requires the participation of 4 parties: A vehicle owner purchases a FASTag from any of the 26 certified issuer banks (such as ICICI Bank, SBI, or Axis Bank) and links it to a prepaid wallet or bank account. At the toll plaza, the transaction is handled by an acquirer bank – one of 12 banks certified to manage toll-plaza payments infrastructure on behalf of the concessionaire operating that plaza. When the vehicle's tag is read, the acquirer bank sends the transaction to the National Payments Cooperation of India (NPCI), which acts as the central clearing and settlement house, routing the debit request to the correct issuer bank. The issuer bank debits the vehicle owner's account and confirms the transaction back through NPCI to the acquirer, which signals the plaza to allow passage. [21]

The Ministry of Road Transport and Highways (MoRTH), through its nodal agency National Highway Authority of India (NHAI), initiated the development of electronic toll collection. MoRTH set up a committee headed by Nandan Nilekani to study electronic toll collection systems and lay down a road map for the project. [22] This committee recommended the formation of a special purpose vehicle to implement the system, which resulted in the incorporation of the Indian Highways Management Company Limited (IHMCL). IHMCL follows a public-private ownership model: NHAI holds a 41.38% stake, toll concessionaires collectively hold 33.81%, and financial institutions hold 24.81%. [23] Private shareholders include L&T Finance, GMR Highways, Shapoorji Pallonji Roads, and Essel Infraprojects, each holding between 3–8% of total share capital. [24] NPCI – a non-profit company owned by a consortium of major Indian banks – acts as the centralized clearing and settlement house (CCH) for all NETC transactions. It manages transaction routing, ensures interoperability, and certifies issuer and acquirer banks that participate in the FASTag ecosystem.

[DRAFT — compiled at 2026-05-08 7:27; not for distribution]

DPI	Ownership	Governance	Economic model
FASTag	Public-private (IHMCL); NPCI as clearing house	MoRTH/NHAI policy; IHMCL operations; NPCI member rules	Govt-subsidised; fixed per-transaction fees to banks and NPCI
Aadhaar eKYC	Government (UIDAI, statutory authority under MeitY)	UIDAI bilateral agreements; NPCI Setu adds aggregator layer	Govt grant-funded; ₹1–3 per transaction + KUA license fees
DigiLocker	Government (NeGD under DIC/MeitY); built in-house	DigiLocker Rules; MeitY in dual operator-regulator role	Grant-funded, free for users; ₹2 lakh + ₹2 cr DLSP entry barrier
Account Aggregator	Decentralised; 17 licensed AAs (16 private, 1 government)	RBI Master Directions; ReBIT specs; Sahamati industry alliance	Free for users; per-transaction fees to FIUs (lenders)
Bharat Connect	NPCI (non-profit) owns NBBL (commercial subsidiary)	RBI authority; NBBL operations; advisory Steering Committee	Commercial; ₹8,000+ cr revenue, 32% profit margin (FY24)
UPI	NPCI (Section 8, bank-consortium owned)	RBI under PSS Act; NPCI operations; UPI Steering Committee	No MDR; ₹3,600+ cr govt subsidies (2021–24); TPAPs monetise data

Table 1: Institutional structure of the six DPIs evaluated.

4.1.2 Development and deployment

Early attempts to operationalize the system relied on a centralized clearing-house model. In 2014, ICICI Bank was selected through a bidding process to act as the central clearing house provider and to distribute RFID tags while managing clearing and settlement between toll operators. [25] However, concerns soon emerged regarding the viability of the bid and the slow pace of implementation. ICICI had issued only a limited number of tags nationwide, while Axis Bank (who was later permitted to offer the same services) never commenced operations. By 2015, the Ministry canceled the model entirely, citing slow adoption and concerns that key transaction data remained outside government control. [25]

The project was subsequently redesigned to adopt a more distributed architecture. Under the revised model, multiple banks could issue FASTags to customers and partner with toll plaza operators, while the NPCI was designated as the centralized clearing and settlement house for all toll transactions under the NETC framework. There is no publicly documented evidence of formal public consultations during FASTag's design or deployment; the system was conceived and implemented through government directives (MoRTH/NHAI), with private-sector participation structured through IHMCL's equity model and bank certification processes rather than through open stakeholder engagement. [25]

Development and deployment responsibilities are now distributed across several actors. Private technology vendors serve as system integrators to configure toll plaza infrastructure, issuing banks manage customer accounts and tag distribution, and acquiring banks work with toll operators to process transactions. [21]

4.1.3 Governance

FASTag's administration reflects a highly networked public-private architecture. Policy authority rests with the MoRTH and NHAI. IHMCL serves as the system operator and policy enforcer, responsible for setting the rules of participation, determining fee structures, and conducting regular compliance audits.

Much of the governance of the actor ecosystem is done through the Procedural Guidelines [26] and the Interface Control Document Manual [27], issued by the NHAI and NPCI. The Procedural Guidelines lay out the roles and responsibilities of the system actors, but most of the adherence is restricted to "members" which are the member banks of the NPCI i.e., the issuers and acquirers. Amongst other things, members are required to comply with money laundering/terrorism financing (ML/TF) regulations including having written ML/TF policies, implement internal monitoring controls and conduct risk assessments. The Guidelines also require members to monitor potentially fraudulent activity. NPCI can suspend/terminate membership

[DRAFT — compiled at 2026-05-08 7:27; not for distribution]

from the NETC system for non-compliance. The procedural guidelines do not have a privacy policy, but instead allocate responsibility to acquirer/issuer to ensure compliance with "privacy related regulations of the government." There is no listed oversight mechanism or sanction for noncompliance. [26] The Interface Control Manual contains technical and transaction specifications, API specs, encryption requirements, dispute management etc. [27]

4.1.4 Economic and business models

FASTag operates on a revenue model, with fixed fees to all the stakeholders involved in the system. Users purchasing a FASTag from an issuer bank typically pay a one-time tag issuance fee (INR 0–100) and a refundable security deposit (INR 200). However, the primary revenue flows occur within the backend toll payment processing chain. Each toll transaction triggers a fixed percentage-based payout to the involved entities. The acquirer bank, issuer bank, NPCI, and IHCML receive 0.13%, 1%, 0.15% and 0.25% of the transaction value respecitively as programme management fee. [28]

These transaction-based payments create clear performance incentives for banks and program operators. Crucially, these payments do not come directly from end-users, as the total toll amount paid remains unchanged (so far,) but are underwritten by the government, making FASTag an example of state-subsidized digital infrastructure. The requirement that users hold a bank account with the issuing bank creates secondary customer acquisition benefits for participating financial institutions.

System integrators and PSPs (payment service providers), while not directly remunerated per transaction, profit from integration services, maintenance contracts, and add-on features (e.g., parking and fuel payment expansions).

4.1.5 Openness

The FASTag system is closed by design, with no open-source components or publicly accessible APIs. Participation is restricted to entities empanelled by NPCI, such as toll plaza operators and issuing banks, who must also have service agreements with IHCML. Their operations are governed by a controlled set of specifications outlined in the Interface Control Document, leaving no scope for external actors to build upon or extend the system. [27] Development and governance remain tightly managed by NPCI and IHCML, with little transparency or openness in how the system evolves. [27]

4.1.6 Coercion

The use of FASTag was made mandatory in January 2021 through amendments to the motor vehicles act framework. [29] Non-compliance with this— either through not having a FASTag or having insuffiecient balance— results in the users having to pay 1.25 to 2 times the toll amount. [30, 31]

4.1.7 Data collection practices

The NETC FASTag system collects and processes a wide range of personal and transactional data. However, the system does not appear to be governed by a dedicated privacy policy. Instead, data practices are primarily regulated through the Motor Vehicles Act (as amended), NPCI-issued circulars, and technical documentation like the Interface Control Manual (ICM).

User data collection To register for a FASTag, users must provide the Registration Certificate (RC) of the vehicle, a passport-size photograph, and KYC documents such as PAN card, driver's license, voter ID, or passport. A mobile number is also collected and verified via OTP. Additionally, the FASTag must be linked to an existing financial account (savings, current, prepaid, card, or UPI) for which KYC norms have already been completed. [32]

Usage data and metadata When users pass through a toll plaza, multiple devices generate and collect data: RFID readers capture the Tag ID, TID (transponder ID), and user memory; Automatic Vehicle Classification (AVC) systems determine the vehicle class; Weight-in-Motion (WIM) sensors record vehicle weight; and image capture systems photograph the vehicle. [27, 26]

[DRAFT — compiled at 2026-05-08 7:27; not for distribution]

This data is transmitted to the plaza server, and then to the acquirer bank and NETC mapper. NETC Mapper is a repository of Vehicle Information, Vehicle Owner Information, NETC FASTag Details, Bank Information and the Exception List. The transmitted data is validated and mapped to the information stored in the Mapper. Each transaction is logged with a timestamp and toll location, and toll operators are expected to retain logs for up to three months. These logs are mandated for "audit and dispute purposes" but is not otherwise protected or restricted from sharing in any manner. It is unclear who can access/request this data and when, but the Interface Manual details how fraudulent transactions must be addressed, and one of these – cloned tag transactions – require an assessment of where the different transactions for one tag processed, and whether the tag could have travelled between those two points within the time of transactions .Presumably, this is a scenario in which location and time data is shared, but the governing documents are not prescriptive in when and for what reason this may be done. [27, 26]

4.1.8 Data sharing and linking with other databases

Within the NETC system, data flows from the toll plaza operator to the acquiring bank, NETC mapper, issuing bank, and back, enabling toll deduction and SMS notification. [27, 26] Outside the NETC system, FASTag data has been leveraged by different agencies, both state and national, and integrated into other systems, to aid in surveillance and enforcement. Some current uses include:

- **Odisha State Transport Authority** for vehicle insurance enforcement, using an e-detection system installed at toll booths where data is collected through FASTags. [33]
- **GST authorities** Through the integration of FASTag into the recently implemented e-way bill system to allow real-time tracking of commercial vehicles. In 2021, under the new initiative IHMCL signed an MoU with Goods and Services Tax Network (GSTN), ULIP and NATGRID for the integration of their system with FASTag. This integration will help the respective authorities to track and trace FASTag vehicles. [34]
- **VAHAN** India's national vehicle registration database, which now verifies and stores FASTag data including registration number, chassis number, and engine number during the application process. [35]

This is not recorded or prohibited in any of FASTag/NETC's documents, suggesting there may be many more applications of FASTag's infrastructure/data in the future.

4.1.9 Data security and privacy

There is no overarching framework requiring disclosure of data breaches across the NETC ecosystem. Instead, responsibility lies with the individual entities that collect or process data (e.g., issuing banks, toll plaza operators). There are no published protocols or transparency requirements regarding data governance. However, instances of data leaks have been reported:

- In 2021, sensitive information such as vehicle class, tag ID, and digital signature data was reportedly leaked from toll plaza operators. [36]
- In 2024, ICICI Bank's FASTag data allegedly appeared on the dark web. [37]

4.2 Aadhaar eKYC

4.2.1 Introduction and ownership

The Aadhaar eKYC system was introduced by the Unique Identification Authority of India (UIDAI) as an extension of its basic authentication service, allowing identity verification to move beyond a simple "yes" or "no" response. Unlike authentication, which only confirms whether a submitted Aadhaar number and biometric/OTP match the records, eKYC enables the transmission of demographic data, such as name, date of birth, and address, from the Aadhaar database to authorized service providers. This marked a significant shift in the Aadhaar framework, as it became the only instance in which personal data is transmitted out of the system rather than simply verified within it.

[DRAFT — compiled at 2026-05-08 7:27; not for distribution]

The Aadhaar ecosystem is entirely owned and operated by UIDAI, a statutory authority established under the Ministry of Electronics and Information Technology (MeitY). The NPCI is also a prominent actor in the eKYC system, through its eKYC "Setu" platform, which acts as a technology layer facilitating secure transmission of KYC data between UIDAI and authorized requesting entities such as banks, telecom providers, and fintech companies. [38]

4.2.2 Development and deployment

The stated motivation behind extending Aadhaar's functionality to eKYC was financial inclusion: before Aadhaar, paper-based KYC verification for opening bank accounts was costly, slow (often taking days or weeks), and discouraged service providers from expanding into underserved populations. [39] The RBI formalised Aadhaar eKYC's legal basis through a circular issued on 2 September 2013, directing banks to accept online Aadhaar e-KYC as an "Officially Valid Document" under the Prevention of Money Laundering Act (PMLA), 2002. [40] Banks were required to enter into KYC User Agency (KUA) agreements with the Unique Identification Authority of India (UIDAI) and deploy the necessary infrastructure to integrate with the Aadhaar authentication system. [40] There is no publicly documented formal public consultation process specific to the eKYC service, it was instead primarly introduced through regulatory directives.

The eKYC service involves a layered network of actors within the Aadhaar ecosystem. UIDAI operates the central identity infrastructure and manages access to the Central Identities Data Repository (CIDR). [41] Entities that seek to use Aadhaar authentication are designated as Authentication User Agencies (AUAs), while those permitted to access demographic data through the eKYC service are classified as KYC User Agencies (KUAs). [42] These actors may also operate through sub-KUAs, such as regulated intermediaries functioning under an authorized KUA. Connectivity to UIDAI's infrastructure is provided through Authentication Service Agencies (ASAs), which maintain the secure network links required to transmit authentication requests. [42] Although access to Aadhaar authentication services for private entities was restricted in 2018, the framework has since been partially restored, allowing private actors to use Aadhaar-based eKYC on a voluntary and consent-based basis, subject to regulatory approval and compliance with UIDAI's access conditions. [43]

4.2.3 Governance

The Aadhaar e-KYC authentication ecosystem is formally mediated by the Unique Identification Authority of India (UIDAI), which designates private and public actors as Authentication User Agencies (AUAs), e-KYC User Agencies (KUAs), or Authentication Service Agencies (ASAs). Any public or private agency may apply to UIDAI for permission to act as a Requesting Entity, provided that its intended use of the authentication service falls within the legal purposes permitted under Section 4(4) or Section 7 of the Aadhaar Act. [42, 43] Upon satisfaction of eligibility criteria, UIDAI signs bilateral agreements outlining permitted use cases, technical standards, and compliance obligations.

In practice, this regulatory structure creates multiple chokepoints to access, limiting the number of entities that can directly interface with UIDAI's Central Identities Data Repository (CIDR). To address this, the Ministry of Electronics and Information Technology (MeitY), in 2023, issued a circular establishing a sector-specific aggregator model known as the e-KYC Setu system. [38]

Under this arrangement, the National Payments Corporation of India (NPCI) functions as an ASA for financial institutions regulated by bodies listed under Section 11A of the Prevention of Money Laundering Act, 2002, including the Reserve Bank of India (RBI), the Securities and Exchange Board of India (SEBI), the Insurance Regulatory and Development Authority (IRDAI), and the Pension Fund Regulatory and Development Authority (PFRDA). [38] Through NPCI's Setu, these regulated entities are permitted to perform Aadhaar-based e-KYC authentication without entering into separate agreements with UIDAI or registering as KUAs. [38]

This model significantly lowers the barrier to entry for private sector actors such as NBFCs, brokerages, and insurance intermediaries, many of whom can now rely on Setu to access UIDAI's authentication services indirectly. Critically, under the e-KYC Setu protocol, authentication is carried out without disclosing the Aadhaar number to the requesting entity. [38] However, NPCI's dual role as both aggregator and ASA centralizes control over access and architecture, with limited transparency into the governance of consent,

[DRAFT — compiled at 2026-05-08 7:27; not for distribution]

data storage, or potential misuse across layers of implementation. Currently, only one agency, HDFC Bank Ltd., is listed as a beneficiary of e-KYC Setu.

4.2.4 Economic and business models

UIDAI receives annual Grants-in-Aid (GIA) from Ministry of Electronics and Information Technology (MeitY) for its operation and development. In 2023-24, UIDAI received a total grant of ₹800 crore, and spent a total of ₹1396 crore, the remaining used from the newly instituted UIDAI fund which includes receipt from services as well as other government funding sources [41].

UIDAI charges private service providers a fee between ₹ 1 and ₹ 3 per eKYC transaction [44]. Additionally, KUAs have to pay a license fee to UIDAI when applying to act as a KUA [45] .

4.2.5 Openness

Despite being framed as a foundational layer of India's digital public infrastructure, the Aadhaar e-KYC system exhibits limited openness in practice. While the authentication and e-KYC APIs are publicly documented, they are not open for unrestricted use or adaptation. Access to the system is tightly controlled by the Unique Identification Authority of India (UIDAI), which requires service providers to undergo a formal application and verification process to be designated as KYC User Agencies (KUAs) [42]. Approved entities must enter into legal agreements with UIDAI, and are subject to registration fees, subscription costs, and per-authentication charges [46]. Although the NPCI's e-KYC Setu initiative aims to streamline onboarding for regulated entities under the Prevention of Money Laundering Act, it still operates as a brokered gateway – limited to institutions already vetted by sectoral regulators. In this sense, the Aadhaar e-KYC infrastructure resembles more of a closed, state-licensed utility than an open digital public good, with participation gated by policy discretion rather than technical openness.

4.2.6 Coercion

While Aadhaar-based e-KYC is officially framed as a voluntary, consent-based mechanism, its use becomes effectively mandatory for individuals seeking access to a range of state welfare schemes. In particular, beneficiaries of government support delivered via Direct Benefit Transfers (DBT) are required to link their bank account with Aadhaar and complete Aadhaar authentication to continue receiving subsidies [47].

This conditionality extends beyond DBT to essential entitlements such as food rations and cooking gas subsidies. In states like Rajasthan, e-KYC through Aadhaar is required for continued enrolment in the Jan-Aadhaar welfare scheme, which consolidates over 30 social benefit programs [48]. Similarly, in Andhra Pradesh and Karnataka, state governments have directed ration card holders to complete Aadhaar e-KYC to remain eligible for Public Distribution System (PDS) entitlements, with strict deadlines announced and periodically extended [49, 50]. Central schemes such as the LPG subsidy program also require Aadhaar authentication, as clarified by recent government press releases [51]. These mandates reframe consent as a condition for access, especially for economically vulnerable populations who may be unable to opt out without forfeiting essential services.

4.2.7 Data collection practices

Under the Aadhaar eKYC system, data is collected and processed at several stages of authentication. When a resident initiates authentication through a KUA (KYC User Agency), the system captures their Aadhaar number (or alternatives such as a Virtual ID or UID token) together with biometric data or a one-time password, which is then encrypted into a "PID block" [39]. In response, the KUA receives demographic details such as name, date of birth, gender, address, and mobile number, along with the Aadhaar number or token, a photograph, and a unique alphanumeric code linked to the transaction. [39] Each eKYC transaction also generates metadata, including the transaction identifier and response codes, which AUAs (Authentication User Agencies) are required to store for dispute resolution. [39] Authentication logs are created at multiple levels: KUAs must retain logs of requests and responses, while UIDAI itself keeps authentication logs for six months, covering both request data (including the PID block) and response data. [52] UIDAI's regulations prohibit the storage of biometric data beyond the real-time transaction, and also forbid the storage of

[DRAFT — compiled at 2026-05-08 7:27; not for distribution]

authentication purposes or additional metadata beyond what is needed for processing. [52] Further, AUAs are barred from using or retaining demographic data obtained through the eKYC API beyond the permitted "time to live." [52] Nonetheless, demographic, biometric, and KYC information remain stored in the CIDR (Central Identities Data Repository). [39]

4.2.8 Data sharing and linking with other databases

The Aadhaar eKYC system is a part of the larger Aadhaar ecosystem, particularly through requiring Aadhaar authentication. It does not however permit third party sharing of data through KUAs/requesting entities.

4.2.9 Data security and privacy

The Aadhaar system has faced repeated allegations of data breaches and unauthorized access over the past decade. These have ranged from reports of Aadhaar-linked personal information being sold online, [53] to cases where cloned biometrics were allegedly used to siphon money from bank accounts. [54] In response, the UIDAI has consistently denied any compromise of the Central Identities Data Repository (CIDR), asserting that no breach has occurred at the core database. [55, 56] However, this denial leaves open a significant accountability gap. UIDAI has not addressed whether Aadhaar-linked data in other government systems seeded with Aadhaar numbers, or data in transit between requesting entities and the CIDR, may have been accessed or leaked. By narrowly defining what constitutes a breach, the authority distances itself from incidents across the wider Aadhaar ecosystem, despite these being integral to how the system functions in practice.

This fragmented model of responsibility, where the UIDAI governs the CIDR but distances itself from the broader digital infrastructure that relies on Aadhaar, creates a governance vacuum. With multiple state central government schemes, public sector entities, and regulated private actors employing Aadhaar for eKYC services, there is no comprehensive framework to assign liability or ensure redress in the event of a breach outside the CIDR. There is not even a requirement to notify the Aadhaar holder in the event of a breach; notifying UIDAI fulfils breach notification compliance. Without meaningful transparency obligations or breach notification requirements, it remains unclear how individuals can find out if their data was leaked, let alone seek remedy.

4.3 Digilocker

4.3.1 Introduction and ownership

DigiLocker is an initiative of the Government of India, launched in 2015 by the Ministry of Electronics and Information Technology (MeitY), as part of the Digital India program. [57] It serves as a platform that allows citizens to store, access, and share digital versions of official documents such as driving licences, PAN cards, educational certificates, etc. By enabling issuers (government departments, universities, insurance companies) to provide digitally signed documents and requesters to access them on demand, DigiLocker aims to eliminate the need for physical copies and increase trust in digital records. [57]

The system is owned by the Government of India through the Digital India Corporation (DIC), [58] with the National e-Governance Division (NeGD) – an independent business division within DIC – responsible for its design, development, and overall oversight. [59] DigiLocker has been built almost entirely in-house by a team of government personnel, supplemented by selected private technology partners. [60]

4.3.2 Development and deployment

DigiLocker began as a state-level experiment in Maharashtra in 2014, where a small government team built a basic Aadhaar-linked document storage application on the state cloud. [61] The prototype was transferred to the central government through an MoU, and a core team within the National e-Governance Division (NeGD), comprising government technologists and a private consultant, scaled it into national infrastructure under the Digital India programme. [61] The team faced a critical design choice: the Digital Locker Rules had originally envisioned a federated ecosystem of licensed Digital Locker Service Providers (DLSPs), in which multiple private operators would offer competing locker services under a common regulatory framework. [62]

[DRAFT — compiled at 2026-05-08 7:27; not for distribution]

Instead, the team chose to build a platform in-house, to meet requirements of verification, integration with hundreds of departments, and Indian security compliance. [62] No DSLPs have emerged as of yet, leaving MeitY in a dual role as both operator and regulator of the DigiLocker ecosystem. [62] There was no formal public consultation process for DigiLocker's design or deployment.

The platform was launched in 2015, and amendments were made to India's Information Technology Act in 2017 to give DigiLocker documents the same legal weight as physical originals. Adoption was largely driven through bilateral partnerships with individual issuing agencies – such as the Central Board of Secondary Education, to issue marksheets and academic certificates – rather than through legislative mandates or structured stakeholder engagement. [61, 62] The DL system relies on three key categories of participants: issuers, who provide verifiable digital documents in machine-readable formats (such as universities, government departments, or licensing authorities); requesters, who access and verify these documents (such as employers, service providers, or verification agencies); and service providers, who build and maintain the portals, access gateways, and repositories that form the infrastructure backbone of DigiLocker. [63] The platform is hosted on ownCloud, with every citizen getting 1GB of free cloud storage. [64]

4.3.3 Governance

The DigiLocker ecosystem is anchored in the DigiLocker Rules, issued by MeitY, which provide the legal foundation for the system. [65] These rules establish the DigiLocker Authority (DLA) as the nodal body responsible for maintaining the platform, authorizing and certifying participating service providers, and setting compliance requirements. [65] Critically, the rules give legal equivalence to digitally signed electronic documents issued through DigiLocker, ensuring that such documents must be treated on par with their physical counterparts (for instance, a voter ID issued via DigiLocker must be accepted as valid proof of identity). [65]

While the Rules create the basic framework, much of the governance detail is left to be determined by the DLA and the Government of India through standards, technical specifications, and contractual arrangements. The DigiLocker platform's Terms and Conditions of Use apply separately to issuers, requesters, and end users, defining their roles, obligations, access controls, and the conditions under which their participation can be terminated or suspended. [66]

The system's technical underpinnings are set out in the DigiLocker Technical Specifications (v2.3, 2015), which define the overall architecture and prescribe a standardized mechanism for issuing, storing, and sharing government documents in electronic and printable formats. [67] These specifications require unique identifiers for issuers, requesters, and documents, set out the flow of data within the system, and specify security and privacy compliance requirements. [67] They are complemented by detailed Issuer and Requester APIs that all ecosystem participants must implement, as mandated through the Rules, Terms of Use, and individual contracts or MoUs. [68]

The DL Partner Onboarding SOP further operationalizes governance by specifying the eligibility criteria, evaluation, verification, technical integration, and testing processes for organizations seeking to join the ecosystem. [69] It also formalizes legal compliance through MoUs, contracts, and other agreements, ensuring that partners adhere to applicable data protection regulations and technical standards. [69]

4.3.4 Economic and business models

The DigiLocker ecosystem operates primarily as a government-funded public service. Its core development and maintenance are supported through annual government grants. [70] While the DigiLocker Rules permit the service provider charging of fees from users, [65] the government-run DigiLocker application does not currently levy charges for regular services, only for select premium features. Revenue generation is more apparent on the partner-integration side of the ecosystem. Digital Locker Service Providers (DLSPs) are required to pay a one-time integration or license fee of INR 2,00,000 for a fresh application and INR 40,000 for renewal. In addition, applicants must submit a performance bond in the form of a banker's guarantee of at least INR 2 crore, valid for six years. [71] These financial requirements potentially act as an entry barrier for service providers, and could even explain the complete lack of alternate DL service providers, even nearly 8 years after opening it up to private participation. [62]

[DRAFT — compiled at 2026-05-08 7:27; not for distribution]

4.3.5 Openness

The DigiLocker ecosystem is designed to support a multi-provider model by allowing repositories to be operated either by issuers themselves, by a central government-provided repository, or by authorized third-party providers. Similarly, the gateway that facilitates document exchange can, in principle, be provided by a third party as long as it complies with the DigiLocker Technical Specifications (DLTS). In practice, however, such alternatives have not emerged, and there continue to be no other DLSPs in the ecosystem. Access to DigiLocker routes back through the official DigiLocker platform or mobile application.

The system relies on open standards, which provide a standardized architecture and API specifications to enable interoperability across repositories and requesters, theoretically allowing both public and private entities to participate in the ecosystem. This design is intended to foster competition and user choice by allowing issuers and requesters to select the repository or gateway that best meets their needs.

However, DigiLocker does not make its APIs fully accessible or open, disallowing unrestricted use/adaptation. Participation in the system – whether as a repository, issuer, or requester – requires formal onboarding, verification, and certification. Additionally, user access remains limited to Aadhaar holders, which constrains universal accessibility and excludes residents without Aadhaar numbers from using the system. [67]

4.3.6 Coercion

Use of DigiLocker is voluntary for individual users, and there is no legal requirement to create an account. However, the system has been made mandatory for other actors within the ecosystem. All government departments and institutions that offer citizen-facing services have been directed to integrate their systems with DigiLocker to enable digital issuance and verification of records. [72, 73] DigiLocker has also been designated as the sole National Academic Repository, meaning that all digitized education records must be stored and accessed through this platform. [74] While users are technically free to opt out, there have been instances where DigiLocker was made de facto mandatory for individuals – such as a press note from the Mumbai passport office requiring applicants using Aadhaar for identity verification to do so via DigiLocker. [75]

4.3.7 Data collection practices

The DigiLocker ecosystem collects and processes multiple categories of data to enable its services. This data falls into four main stages: registration, use, data received from other databases, and metadata generated during interactions with the platform.

Data Collected During Registration When a user signs up for DigiLocker, the system collects basic demographic and contact details, including name, gender, mobile number (linked to Aadhaar), email ID, and a photograph fetched from the Aadhaar database. These details form the basis of the user's profile within DigiLocker and enable subsequent authentication and communication. [76]

Data Collected During Use To access documents through DigiLocker, users must provide identifiers specific to the issuer or document type, such as their Aadhaar number, roll number and year of examination (for academic records), or date of birth. Any documents voluntarily uploaded by the user or issued into their DigiLocker account by partner issuers are also stored in the system. [76]

Data Collected from Other Databases DigiLocker integrates with other services and databases, most notably the Aadhaar system, from which it conducts eKYC to verify the user's identity. It also accesses data from authorized issuers (such as government departments and academic institutions), that are stored in the issuers' repositories. [76, 67]

Metadata Collected In addition to user-provided data, DigiLocker collects system-level metadata through its privacy policy, such as IP addresses, domain names, browser type, operating system, date and time of visit, pages accessed, and referring URLs. While the policy states that these data points are not linked to an individual's identity except in cases of unlawful activity, they contribute to system monitoring and security. The platform also generates detailed activity logs, which allow users to review when and with

[DRAFT — compiled at 2026-05-08 7:27; not for distribution]

whom their documents or URIs have been shared. Through the issuer API, the system additionally records document identifiers and classifications (such as whether a document is a caste certificate, driver's license, or marksheet), to enable standardized management and retrieval across the ecosystem. [76]

Data Storage The DigiLocker ecosystem follows a federated storage model, where issued documents are retained in the issuer's repository and accessed through a Uniform Resource Identifier (URI) rather than being centrally stored. [67] When an issuer does not maintain its own repository, a central repository is created for that domain – for example, the National Academic Depository for educational records or the Ayushman Bharat Health Account for health-related data. Users are also allowed to upload self-attested documents into their personal DigiLocker account, which are then stored in the DigiLocker cloud within the allocated free storage space. [67]

Importantly, the DigiLocker gateway is designed only to facilitate transient access to documents and is explicitly prohibited from storing URIs, e-documents, or authentication credentials. Instead, it retains only anonymized audit trails for accountability. [67] However, identity and authorization information, such as demographic details, Aadhaar number, and authentication logs, are stored centrally in DigiLocker's own storage systems. [76]

4.3.8 Data sharing and linking with other databases

By design, DigiLocker functions as a federated platform, connecting multiple document repositories and enabling the exchange of records between issuers, requesters, and users. When a document is issued, it is stored in the issuer's repository and linked to the user's account through a URI (Uniform Resource Identifier). The DigiLocker gateway uses this URI to locate the repository and retrieve the document when requested. [67]

The platform is also deeply integrated with Aadhaar. Aadhaar credentials are used both at the time of registration and during the document issuance process. The DigiLocker APIs recommend that issuers match the demographic details on their certificates with the user's Aadhaar data to ensure that only the rightful owner gains access to their documents. [68] Issuers can also configure their APIs to use Aadhaar-linked parameters – such as Aadhaar number, name, and date of birth – for document identification and seeding. [68] Where Aadhaar seeding is unavailable, other unique identifiers such as driving license numbers may be used. This is similarly true when a requester requests access to a document/certificate. [68]

Outside of the regular operation of the system, DL permits disclosure of data to actors outside the DL ecosystem in certain cases. DigiLocker's Privacy Policy permit the sharing of "personal and usage information" with other organizations if the government (through MeiTY) believes it is necessary to comply with applicable laws or enforceable government requests, prevent fraud or security issues, or protect the rights or safety of users and the public. [76] Similarly, the Terms of Use permit the inspection of metadata – such as file sizes, timestamps, and filenames – to identify potential violations, in response to a lawful request or court order, as well as access to user content in case of judicial authorization. [66] There are no specifications or restrictions on who this may be shared with, or how it is overseen.

4.3.9 Data security and privacy

The DigiLocker ecosystem incorporates audits and system monitoring to secure data. All issuers, requesters, and service providers are required to conduct mandatory annual security audits of their systems, with reports submitted to the DigiLocker Authority or the Government of India within four weeks of completion. [**?** 66] The technical specifications go a step further by requiring repository providers to make access audits publicly available through a URI, enabling at least some degree of transparency into system activity. [67]

Despite these safeguards, breach response mechanisms remain somewhat opaque. The DigiLocker privacy policy states that the system is under continuous security monitoring, including vulnerability scans, traffic analysis, and threat tracking, and promises "swift action" in the event of security incidents. [76] However, there is no clear requirement to notify users directly if their data is compromised. The terms of use impose a 24-hour reporting obligation on issuers and requesters to inform the DigiLocker Authority or the government in the event of a breach, but this duty does not extend to affected individuals. [66]

[DRAFT — compiled at 2026-05-08 7:27; not for distribution]

DPI	Source code	API Openness	Public consultation	Community contributions
FASTag	×	×	×	×
Aadhaar eKYC	×	◐	×	×
DigiLocker	×	◐	×	×
Account Aggregator	◐	✓	✓	◐
Bharat Connect	◐	×	✓	×
UPI	×	×	×	×

✓ yes × no ◐ partial / qualified

Table 2: Openness characteristics of the six DPIs evaluated.

This lack of mandatory user notification has been particularly significant in light of reported vulnerabilities and incidents. For example, researchers have disclosed critical vulnerabilities in the DigiLocker platform that could potentially expose sensitive user data or allow unauthorized access to accounts. [77] While the government has claimed that such issues were swiftly resolved, the absence of a formal, public breach disclosure process makes it difficult to assess the impact or extent of such incidents.

4.4 Account Aggregator

4.4.1 Introduction and ownership

In 2016, the Reserve Bank of India (RBI) introduced Account Aggregators as a new class of Non-Banking Financial Companies (NBFCs). Account Aggregators (AAs) allow users to access all their financial information (from banking, insurance and investments) in one place, and facilitate sharing of this data with other financial institutions. [78] The AA framework has been recognised (with the Data Empowerment and Protection Architecture) as "a foundational Digital Public Infrastructure (DPI) serving as the data exchange layer, complementing the identity (Aadhaar) and payments (UPI) layers." [6, 79]

Account Aggregators are governed by the RBI, and the Master Directions issued by the latter outline the core aspects of their governance and operation. All AAs are companies that apply to the RBI to get registered as such. ReBIT (Reserve Bank Information Technology Pvt Ltd), a wholly-owned subsidiary of the RBI, was authorised to develop technical standards for AAs. [80]

As such, the AA framework is not a DPI with a central service. Instead, the regulations and specifications allow for information sharing with a consent-based framework. Account Aggregators themselves are usually private companies providing these services via mobile applications.

4.4.2 Development and deployment

In 2016, the RBI sought stakeholder comments on the Draft Regulatory Framework for Account Aggregator Companies to Facilitate Consolidated Viewing of Financial Asset Holding. [81] It envisaged the creation of account aggregators as a new class of NBFCs. The RBI issued Master Directions in 2016 to the same effect under Section 45J of the RBI Act, [80] which gives broad powers to the RBI to issue directions "in the public interest or to regulate the financial system of the country." Notably, the scope of AA activities expanded between these two events: the draft Directions envisioned AAs as providers of consolidated account views to customers; the final Directions also see them enabling data-sharing between financial institutions. [82]

The AA Master Directions provide a framework for the governance of AAs, while the API and specific details are published by ReBIT. [83] The Regulations specify three types of entities associated with AAs.

- A Customer is simply an individual end-user of an AA application.
- A Financial Information Provider (FIP) is a financial institution (bank, NBFC, asset management company, insurance company, etc.) that holds customer financial information and shares it upon request.

[DRAFT — compiled at 2026-05-08 7:27; not for distribution]

- A Financial Information User (FIU) is an entity registered with and regulated by a financial sector regulator that requests and receives customer financial information through an AA.

The usage of the terms FIP and FIU is largely dependent on context. The Master Directions require that "regulated entities of the Reserve Bank joining the Account Aggregator ecosystem as [FIU] shall necessarily join as [FIP] also, if they hold the specified financial information."

17 entities have been granted the NBFC-AA license in India. [84] As of September 2025, 54 financial institutions were live as FIPs and 650 institutions live as FIUs – with more than 223.32 million users having already linked their accounts using an AA. [85]

Sahamati, an industry alliance, is also now heavily involved in the development of the AA ecosystem. They regularly publish updates about usage of AA, and guidelines and best practices for companies and developers.

4.4.3 Governance

The RBI is the main regulating entity for AAs, with the Master Directions providing the overarching framework for operations of AAs. [83]

AAs must be registered by the RBI through an application process. Some requirements for AAs include, but are not limited to, that the applying entity must be a company with over 2 crore rupees in funds, and have 'fit and proper' promoters. AAs are granted a Certificate of Registration if the RBI is satisfied with the application and implementation.

RBI may cancel this Certificate of Registration under certain conditions (failure to comply with regulations or directions, non-operation or ineligibility, failure to maintain accounts or failure to disclose its financial position). Changes in shareholders or ownership must be approved by RBI. The Bank may, at any time, inspect any AA as it deems fit. These, among other requirements, are listed in the Master Regulations. [83]

AAs are strictly proscribed in three ways by Section 5 of the Master Directions. First, in terms of functionality, AAs can not facilitate actual financial transactions. Second, AAs cannot store any customer's information, i.e., they should enable the sharing of financial information from FIPs to FIUs. Finally, AAs shall "not undertake any other business other than the business of account aggregator." [83]

As mentioned earlier, AAs are counted as NBFCs. RBI regulates NBFCs in a tiered model based on scale and risks, with AAs identified as Base Layer NBFC. This means that regulations applicable to Base Layer NBFCs also apply to AAs.

The RBI, in March 2025, additionally introduced a Framework for recognising Self-Regulatory Organisations (SROs) for the Account Aggregator Ecosystem. [86] Ostensibly, this move is to officially recognize organizations like Sahamati that are already playing a leading role in standardisation, best practices, compliance and certification.

4.4.4 Economic and business models

The AA framework by itself does not operate on a profit model, but particular AAs are permitted to charge users a fee. In practice, however, most AAs are free-to-use for users, and instead charge FIUs a small fee per transaction. [87] Note again that RBI prohibits AAs from undertaking any business apart from the AA business. [83]

All currently registered AAs are private for-profit companies. There is just one exception, the NeSL Asset Data Limited (NADL), which is a Union government company.

FIUs and FIPs are for-profit entities usually (banks and financial institutions). Technology Service Providers (TSPs) that offer implementations and modules for AAs are also usually for-profit companies.

A large factor in the growth of AAs has been its use by lenders to access bank and financial information of potential borrowers. [88] According to Sahamati, "unsecured lending (INR 426 billion) is driving usage in the AA ecosystem." [89] A RBI educational resource also mentions that AAs "substantially reduce the time for loan processing." [90]

4.4.5 Openness

Account Aggregator is not a centralized service, and therefore, there is no central codebase that could be open-sourced *per se*. ReBIT that is responsible for developing the technical specifications has openly

[DRAFT — compiled at 2026-05-08 7:27; not for distribution]

published API specifications, including those for managing consent in AAs, and for the functionalities of FIUs and FIPs. Together, they encompass they provide for the majority of the feature set of most AAs. These specifications are updated are regularly, but as far as we can tell, not openly collaborated on. For example, when in 2023, ReBIT published a major update to the AA specifications that players had to start complying with, there was no consultation or contribution period open to the public. [91]

While the AA framework itself has (and structurally cannot have) any open source code, there is an evolving open source community contributing to the proliferation of AAs. For instance, there are open source libraries available for FIUs and account management on AAs. [92, 93] Some AA operators and TSPs like Setu and Finvu also provide public sandbox environments. [94, 95] While there does not seem to be a way to contribute directly to the core AA specifications and infrastructure, the aforementioned repositories do seem open to public contributions.

As seen through the ecosystem, the industry alliance Sahamati plays a leading role in making additional technical specifications and guidelines ("interpreting the [regulations] high-level directions/specifications and crafting lower-level procedural decisions, that are understood and implemented uniformly by all AA participants.") public, including best practices for API security and FIU-AA interaction on user devices. Deployed infrastructure used by many players is also maintained by Sahamati: the Central Registry and Token Server, a common directory of AA participants that provides for discovery of account information and other metadata, has public documentation but the actual infrastructure code is not open-source. Sahamati organises itself into steering committees and working groups that work on these resources; contributing to them directly, however, remains open to its members only. [96]

4.4.6 Coercion

The use of AAs is voluntary, and not mandated by law. No practice around coercing citizens into using Account Aggregators seems to have arisen either. At the level of system use, the Master Directions are quite clear in noting that an AA "shall provide services to a customer based on the customer's explicit consent." [83] A complete consent architecture is laid out in the Regulations. AAs are becoming a model of consent.

That said, given the ease with which financial institutions can process loans, there is an emerging practice of offering of better borrowing rates if a customer provides information with AAs.

4.4.7 Data collection practices

Section 6 of the Master Directions sets out a consent architecture. Pertinently, the Directions mandate all AAs to have a Citizen's Charter that "explicitly guarantees protection of the rights of a customer." AAs are not permitted to keep or retain the information acquired from FIPs. AAs are also not allowed to access or retain any credentials relating to such accounts. Any use of financial information of customers is not allowed by AAs, [83] essentially restricting their role solely to facilitating the exchange of financial data.

Regardless, AAs have their own privacy policies and user flows. Typically, AA apps are asking for mobile numbers and verify the number using a One-Time-Password. Our preliminary analysis of privacy policies of popular AA apps indicates that many apps collect other user information, including email addresses, device information, connection details, etc.

4.4.8 Data sharing and linking with other databases

As described above, the primary role of AAs to facilitate the sharing of information across financial institutions on behalf of a user. AAs are not permitted to share any "information that it may come to acquire from/ on behalf of a customer without the explicit consent of the customer." AAs also cannot not use the third-party services for the main application. [83]

The Directions describe the details of consent artefacts. FIUs getting information through AAs "shall not be use [...] or disclose [it unless] as may be specified in the consent artefact." Such consent can also be revoked by the user. [83]

The Master Directions do not mandate linking AAs with a person's Aadhaar. The Directions require AAs to perform customer identification, but leave the mechanism to the AA. AAs, being NBFCs, must

[DRAFT — compiled at 2026-05-08 7:27; not for distribution]

comply with the broader KYC Directions which govern all RBI regulated entities. Aadhaar can be used for such KYC.

4.4.9 Data security and privacy

The Directions require AAs to build in "adequate safeguards [to ensure protection] against unauthorised access, alteration, destruction, disclosure or dissemination of records and data." The Directions also mandate information security audits and compliance with standards issued by ReBIT. [83]

While the Master Directions essentially confine AAs to perform data exchange in circumstances consent is explicitly provided for, reportage has documented AA applications obtaining consent to access bank statements for periods of up to eight years, with monitoring frequencies as high as once per day. [97] These practices highlight a structural gap in the AA framework: while the Master Directions prohibit FIUs from using data "except as may be specified in the consent artefact", no mechanism exists to monitor FIU usage of data after it leaves the AA. [82] While ostensibly consent-based to begin with, such practices raise concerns about the use of AAs as surveillance tools for financial and fin-tech companies.

There does not seem to be any vulnerability disclosure program or bug bounty specifically for the Account Aggregator ecosystem standards or applications. ReBIT has published a whitepaper on Responsible Vulnerability Disclosure as general guidance for the financial sector, but as a non-binding white paper. Individual Account Aggregator companies may have their own vulnerability disclosure policies. Since AAs are NBFCs, they are required to report security incidents to the RBI. [98]

4.5 Bharat Connect

4.5.1 Introduction and ownership

Bharat Connect, formerly known as the Bharat Bill Payment System (BBPS), is India's interoperable bill-payment infrastructure. It was established under the *Payment and Settlement Systems Act, 2007* (PSS Act, Act 51 of 2007) [99] and regulated through RBI Circular 940/02.27.020/2014-15 (28 November 2014) [100]. The current framework is the *RBI Master Direction (Bharat Bill Payment System) Directions, 2024* (RBI/DPSS/2023-24/111, effective 1 April 2024) [101]. The RBI granted NPCI *in-principle* approval to act as the Bharat Bill Payment Central Unit (BBPCU) via Press Release 2015-2016/1234 [102]. The system was rebranded as *Bharat Connect* in 2024.

Ownership is structured as a two-tier corporate arrangement. The *National Payments Corporation of India* (NPCI) is the apex entity, incorporated as a Section 8 (non-profit) company under the Companies Act 2013 [103]. NPCI created *NPCI Bharat BillPay Limited* (NBBL) as a wholly-owned commercial subsidiary that now operates the platform day-to-day. Below NBBL sit two classes of participants: *Bharat Bill Payment Operating Units* (68 authorised entities comprising 60 banks and 10 non-bank entities) and an agent layer of over 700,000 active touchpoints serving as the customer-facing network [101].

The conceptual development of Bharat Connect was led by the RBI, the *G. Padmanabhan Committee* (2013) and the *Giro Advisory Group*, which recommended the tiered structure adopted in the final design [104, 105, 106]. A structured public comment process accompanied the design phase: draft guidelines were published on 7 August 2014, and the final guidelines were issued based on the public comments received [107].

4.5.2 Development and Deployment

NPCI served as the primary technical development agency, building Bharat Connect on a "unified transaction processing platform [...] processing over 8 billion API calls daily" designed for population-scale use [108]. NBBL is solely responsible for clearing and settlement. The PSS Act prohibits any Technology Service Provider (TSP) from handling funds [101]. Certified TSPs (e.g., Setu, PayU, Juspay, and BillDesk) connect through the *NBBL Developer Program* [109], and API specifications are available on the NPCI portal, though access requires NPCI certification [110].

Deployment followed a phased rollout: the BBPS pilot launched in 2017 in select cities and states, expanding nationally by 2019. The 2024 Master Direction significantly expanded mandatory scope, specifying that "any entity, other than a biller, operating a system for payment of bills outside the scope of BBPS is

[DRAFT — compiled at 2026-05-08 7:27; not for distribution]

a 'payment system' under Section 2(1)(i) of the PSS Act 2007 and will require authorisation" [101]. This represents a formal shift from voluntary to mandatory participation for all in-scope bill-payment service providers.

Operationally, NBBL sets technical and business standards, certifies participants, and guarantees settlement [101]. Customer Operating Units (COUs) provide consumer-facing interfaces. Biller Operating Units (BOUs) onboard and conduct due diligence on billers. Agent institutions extend reach to unbanked populations [111]. Non-bank BBPOUs are required to maintain an escrow account with a commercial bank exclusively for BBPS transactions, and their payment operations are treated as a "designated payment system" under Section 23A of the PSS Act [101].

4.5.3 Governance

The RBI is the ultimate regulatory authority, responsible for authorising and supervising all system participants, conducting audits and compliance monitoring, and acting as the dispute-resolution authority [99, 101]. Below the RBI, NBBL performs day-to-day operational governance: rule-making, technical standard-setting, and the provision of a consumer-dispute framework mandated by Section 6(a) of the 2024 Master Direction [101].

Stakeholder deliberation is channeled through the *BBPS Steering Committee* (a 15-member body with NBBL as a permanent member), which is responsible for project planning, business expansion, fee determination, and advising on implementation standards [111]. Current committee membership is publicly listed [112]. However, the committee's mandate is primarily advisory and deliberative rather than independently supervisory, and there is no independent board or parliamentary committee with oversight powers specifically over BBPS operations.

Bharat Connect success metrics emphasise system availability (e.g., 99.5% uptime requirement), settlement speed (e.g., T+1 realization), national network coverage (e.g., over 700,000 agent touchpoints and over 22,000 billers), and aggregate adoption is tracked via the *RBI Digital Payment Index* [113]. Private-sector participation is incentivised through revenue-sharing commissions, reduced integration costs through a single-platform biller aggregation, and government subsidies (e.g. the Union Budget 2024 allocated funds for digital payment incentive schemes) [114].

Checks on future scope-creep in Bharat Connect are limited. The 2024 Master Direction expanded rather than narrowed BBPS's regulatory perimeter, and no statutory provision explicitly constrains the purposes for which transaction data collected under BBPS may subsequently be used [101].

4.5.4 Economic and business models

Bharat Connect operates through a hybrid economic model: NPCI is a Section 8 non-profit, but its subsidiary NBBL is an explicitly commercial entity. NBBL reported total revenue exceeding ₹8000 crore in FY2023–24, yielding a net profit over ₹2,000 crore and a profit margin of 31.82% [115]. Payment services account for 99.8% of operational revenue and the remainder derives from certification fees and membership charges [115]. NBBL also generates investment income from the Settlement Guarantee Mechanism (SGM) which holds contributions from member banks, alongside a Risk Cover Reserve and a Technology Reserve [115].

Private Operating Units (e.g. PayTM, PhonePe, Google Pay, Amazon Pay, CRED) and major private sector banks generate revenue through per-transaction fees, cross-selling financial products, and merchant acquisition commissions [109].

Academic research has raised concerns that payment behaviour data generated on the platform is used to build credit profiles for consumers, constituting a form of data monetisation beyond the stated bill-payment purpose [116].

Government-funded programs underpin parts of the ecosystem: the Digital India Programme (2015) provided foundational infrastructure support, and successive Union Budgets have funded payment-adoption incentive schemes [114].

4.5.5 Openness

Bharat Connect's openness profile is limited. The core platform source code is not publicly available. NPCI has released only one small open-source component: the Falcon Project [117]. No other component of the

[DRAFT — compiled at 2026-05-08 7:27; not for distribution]

core BBPS transaction-processing infrastructure is available openly.

API access requires NPCI certification and operates over a managed network. Documentation is only available to certified partners through NPCI's portal [110]. The Nfinite Platform serves as an API playground for certified TSPs to test integration [109]. Bharat Connect constitutes a *controlled ecosystem* rather than an open one.

There is no public operational status dashboard or real-time uptime reporting. The system maintains documented 99.5% uptime requirements standards, and participants submit daily transaction reports to the RBI, but none of these data are publicly accessible [101].

Community participation in design or development decisions is not facilitated: no open mailing lists, public issue trackers, or community governance mechanisms exist beyond the formal Steering Committee [112].

4.5.6 Coercion

There is no statutory mandate requiring consumers to use Bharat Connect. Consumers retain the option to pay bills through proprietary biller portals, bank branches, or other channels. However, the 2024 Master Direction introduces mandatory participation for *service providers*: any entity operating a bill-payment system within the defined regulatory scope must obtain RBI authorisation, and non-compliance results in a prohibition from offering bill-payment services [101]. This effectively compels all significant bill-payment intermediaries to route transactions through BBPS infrastructure, narrowing competitive alternatives for consumers over time.

Srikanth et al. documented instances of what can be characterised as coercive data practices: several BBPOUs (including PayTM, PayUMoney, Google Pay India, and HDFC Bank) were found to be retrieving consumers' utility bill data without explicit, transaction-specific consent [116]. Complaints were filed with the RBI Board for Regulation and Supervision of Payment and Settlement Systems regarding the auto-fetching of utility bill payment data even after consumers had uninstalled the relevant applications [116].

These incidents indicate that, even where formal consent mechanisms exist on paper, implementation by participating operating units has not consistently respected consumer autonomy.

4.5.7 Data Collection Practices

Data collection across the BBPS ecosystem is governed by the NPCI Privacy Policy and the *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011* [118], and RBI operational guidelines.

At registration and during transactions, the system collects: personal identifiers (e.g., name, mobile number, email address), government-issued identifiers (e.g., Aadhaar number, PAN number), payment credentials (e.g., OTP, PIN, passwords), financial account details (e.g., account numbers, beneficiary details) and transaction metadata (e.g., reference numbers, timestamps, amounts, originating and destination system identifiers) [119]. The procedural guidelines classify customer information into sensitive, private, and non-sensitive tiers, mandating encryption and hashing for transaction integrity [111]. Beyond registration data, usage generates a rich behavioural record: bill-payment frequencies and categories, geographic signals via IP address, device fingerprints, session-duration data, and payment-method preferences.

Anti-money laundering obligations under the RBI KYC-AML Circular (RBI-2015-16-42, dated 1 July 2015) additionally require active transaction monitoring for anomalous activity, implying systematic analysis of behavioural patterns [120]. Under CERT-IN Directions (70B, April 2022), all ICT systems must retain logs for a minimum of 180 days [121]. Financial transaction records are subject to longer retention—typically 5–10 years under RBI and income-tax regulations.

Each participating actor (e.g., NBBL, COUs, BOUs, agent institutions) collects data proportionate to its operational role. COUs collect the broadest consumer-facing dataset, BOUs collect biller-facing settlement data, agent institutions collect KYC identifiers and transaction data within their interface role. All entities are bound by the same overarching regulatory framework and CERT-IN logging obligations [101].

4.5.8 Data sharing and Linking with other databases

Data Sharing. The NPCI framework restricts third-party data disclosure to legally compelled disclosures (e.g., statutory obligation, judicial decree, or lawful government authority request) and intra-ecosystem

[DRAFT — compiled at 2026-05-08 7:27; not for distribution]

operational sharing with COUs, BOUs, agent institutions, business correspondents, and certified TSPs [119].

Business-transfer provisions additionally reserve disclosure rights during ownership changes or mergers. Systematic user notification of data sharing is absent. The framework is oriented towards regulatory compliance rather than user transparency.

The Digital Personal Data Protection Act, 2023 imposes enhanced consent obligations, formal Data Fiduciary registration, mandatory Data Protection Officer appointment, and annual data-protection impact assessments [122].

Data Linking. Bharat Connect occupies a central position in NPCI's broader identity-linked payment ecosystem. Two formal integration points are notable:

- *Aadhaar Enabled Payment System* (AePS) links Aadhaar numbers to bank accounts and authenticates transactions via fingerprint or iris biometrics [123].
- *Aadhaar Payment Bridge System* (APBS) uses the Aadhaar number as a financial address for routing government Direct Benefit Transfers, implemented by NPCI in collaboration with UIDAI [124].

In addition to these formal linkages, the system collects multiple cross-service identifiers: Aadhaar number, PAN number, mobile number, bank account number, and email address. Each of these identifiers can correlate a user's BBPS record with their profile across other government and private databases.

Srikanth et al. identified this "cross-system data correlation capability across NPCI platforms" as creating the conditions for comprehensive individual profiling without that outcome being the stated purpose of any single system [116].

Aadhaar integration is documented through UIDAI collaboration agreements and RBI payment system guidelines, and the NPCI Privacy Policy acknowledges the collection of Aadhaar and PAN numbers, but no policy document explicitly addresses the downstream risks of cross-platform correlation [101, 123].

4.5.9 Data Security and Privacy

NPCI publicly discloses a substantial set of security certifications applicable to the BBPS infrastructure: PCI DSS v4.0, ISO 27001:2013 (ISMS), ISO 22301:2019 (BCMS), ISO 27701:2019 (PIMS), and ISO 9001 [125]. NPCI reports use of a zero trust Architecture, a 24×7 Security Operations Centre, endpoint protection, threat intelligence integration, and continuous vulnerability monitoring [125]. The procedural guidelines mandate secure data archival for ten years and reserve penalties for non-compliance with Annexure 8 (Compliance, Risk and Information Security) standards [111]. Despite these stated controls, a 2019 government audit found vulnerabilities including "unencrypted personal data storage," which NPCI stated were "subsequently resolved" [125]. No formal public vulnerability disclosure programme or bug bounty scheme exists and security queries are directed to a generic privacy support email. Under CERT-IN Directions 70B, NPCI must report cybersecurity incidents within six hours [121]. User-facing disclosure of security incidents remains limited.

Our analysis identifies the absence of a public vulnerability disclosure programme, the non-consensual data-use practices documented in the literature, and the Aadhaar linkage architecture as the highest-priority residual risks in Bharat Connect's current security and privacy posture.

4.6 Unified Payments Interface

4.6.1 Introduction and ownership

The Unified Payments Interface (UPI) is a digital payments system that allows users of most banks in India to send and receive payments to each other. It provides infrastructure, standards, and a set of APIs (Application Programming Interfaces) that allows banks and other payment applications to conduct real-time digital payments in an interoperable manner. [126] UPI is operated by the National Payments Corporation of India (NPCI), which maintains technical infrastructure and APIs, and defines standards and processes that allow users to initiate and receive payments through mobile applications, web interfaces, and other digital channels. [127] UPI operates on multiple identifiers to identify users and facilitate payments, including Aadhaar number, virtual payment address (VPA), bank account number, and mobile number. It also relies

[DRAFT — compiled at 2026-05-08 7:27; not for distribution]

DPI	Data collected	Data sharing and linking
FASTag	Vehicle RC, KYC documents, photo, mobile; transaction logs with Tag ID, location, timestamp, weight, vehicle image	Linked to VAHAN, GST e-way bill, NATGRID, state transport authorities; expansion not authorised in governing documents
Aadhaar eKYC	Aadhaar number, biometrics/OTP per transaction; demographic data and photo returned to KUA; UIDAI logs retained 6 months	Aadhaar is the linking identifier across the wider stack; eKYC itself prohibits third-party onward sharing
DigiLocker	Aadhaar-linked profile (name, mobile, photo, email); uploaded and issued documents; system metadata (IP, browser, activity logs)	Federated, URI-based access; deeply Aadhaar-integrated; privacy policy permits broad disclosure on grounds of "law" or "security"
Account Aggregator	Mobile + OTP; AAs prohibited from storing FIP data; AA apps collect device info, email, connection details via own policies	Core function is FIP→FIU sharing via consent artefact; no monitoring of post-share use by FIUs; KYC may use Aadhaar
Bharat Connect	Personal IDs (name, mobile, email, Aadhaar, PAN); payment credentials; financial details; transaction metadata; behavioural records	Aadhaar via AePS and APBS; multiple cross-system identifiers (PAN, mobile, account, email); no policy on correlation risks
UPI	Mobile, device IDs, UPI ID, name, masked bank/IFSC; transaction data, VPA, timestamps, merchant codes; optional location	Distributed across PSPs, TPAPs, banks, NPCI; Aadhaar as onboarding option; mobile number now usable as numeric UPI ID

Table 3: Data collection and sharing across the six DPIs evaluated.

on device binding and two-factor authentication mechanisms (including biometric authentication) to secure transactions. [126] Together, these features position UPI as a foundational payments infrastructure for the nation, aimed at replacing regular cash use for low and medium-value retail transactions and peer-to-peer payments.

4.6.2 Development and deployment

UPI is owned and operated by the National Payments Corporation of India (NPCI), a privately owned, non-profit company constituted under Section 25 of the Companies Act, 1956 (now Section 8 of the Companies Act, 2013). [127] NPCI itself was set up as an initiative of the Reserve Bank of India and the Indian Banks' Association under the Payment and Settlement Systems Act, 2007, to build and operate core payment infrastructure in India. NPCI's ownership structure reflects a consortium model. Its original promoter group comprised ten core banks – six public sector banks and four private/foreign banks – and was subsequently broadened to include a wider set of member banks across sectors. [127] In later phases, shareholding was extended to additional RBI-regulated entities such as payment service operators, payment banks, and small finance banks. [127] This structure places UPI within a hybrid institutional model: privately incorporated and bank-owned, but operating as a systemically important payments utility under close regulatory oversight.

The UPI ecosystem involves multiple layers of actors, coordinated through NPCI's network governance mechanisms. At the centre is NPCI itself, along with its shareholders and the UPI Steering Committee, which brings together representatives from a wide range of participating institutions to deliberate on business, operational, and technical issues affecting the network. [128]

Operationally, Payment Service Providers (PSPs) – typically banks – play a key role by acquiring customers and offering UPI payment services through front-end applications. [126] PSPs may provide their own applications or partner with Third-Party Application Providers (TPAPs), such as fintech companies, that deliver user-facing apps while relying on banks for settlement and compliance. [126] Each transaction typically involves a payer PSP and a payee PSP, alongside two banks acting as the remitter bank (from which funds are debited and which issues and stores the UPI PIN) and the beneficiary bank (to which funds are credited). [126] Additional participants include prepaid payment instrument (PPI) issuers, merchants and other recipients of payments, and end users holding bank accounts with UPI-enabled banks. In a standard person-to-person transaction, up to seven distinct entities may be involved – two TPAPs providing user-

[DRAFT — compiled at 2026-05-08 7:27; not for distribution]

facing apps, two PSPs providing the interface layer, two banks handling the underlying debit and credit, and NPCI itself. [126]

4.6.3 Governance

UPI's governance is anchored in the Payment and Settlement Systems Act, 2007, with the RBI exercising ultimate regulatory authority. [99] UPI was launched by the NPCI in 2016 with explicit approval from the RBI, and NPCI operates the platform as an authorized "system provider" under the Act. [129] This position was reaffirmed by the Delhi High Court in 2023, which held that NPCI –rather than third-party apps such as Google Pay – is the operator of the UPI payment system. [130] While third-party applications facilitate user-facing transactions, they do so by operating through PSP banks and NPCI's infrastructure, and do not require separate authorization from the RBI because they are not themselves payment system providers under the Act. [130]

Operational governance is further specified through NPCI's Procedural Guidelines, which define eligibility, roles, and compliance obligations for participation in UPI. [131] Only entities regulated by the RBI under the Banking Regulation Act, 1949, and authorized to provide mobile banking services may become UPI members. Participating banks must formally commit to complying with NPCI-issued rules, RBI directions, and applicable AML/KYC requirements. [131] NPCI retains broad powers within this framework: it prescribes technical and operational standards, approves the participation of issuer banks, PSP banks, TPAPs, and PPIs, manages transaction processing and settlement, and may conduct audits or call for records from any UPI participant, either directly or through third parties. [131]

Responsibility within the ecosystem is deliberately layered. PSP banks bear primary accountability for onboarding users, authenticating customers, issuing and managing UPI IDs and PINs, engaging TPAPs, and ensuring that all associated applications and systems meet prescribed security and audit standards. [132] Data localization obligations require PSP banks to store all UPI transaction data within India, [133] and data sharing with third parties is prohibited except where mandated by law, in which case prior intimation to NPCI and the bank is required. Liability for data security is similarly divided: NPCI is responsible for data security within the UPI network, while PSPs and banks remain responsible for data once it leaves NPCI's systems, including when operations are outsourced to technology service providers. [132] This model centralizes rule-setting and oversight in NPCI and RBI, while pushing day-to-day compliance, security, and grievance redressal obligations down to regulated banks within the network.

4.6.4 Economic and business models

UPI operates on a hybrid economic model that separates ownership from monetization. While the platform itself is owned and operated by NPCI, a non-profit entity, many of the actors that deliver UPI services – particularly Payment Service Providers (PSPs) and Third-Party Application Providers (TPAPs) – operate on explicitly for-profit models. NPCI's own membership is dominated by commercial banks and private firms, which shapes incentives within the ecosystem even as the core infrastructure is framed as a public utility.

Direct transaction-based revenues have been progressively constrained. Until 2020, PSPs and TPAPs were permitted to charge merchants a Merchant Discount Rate (MDR) on UPI transactions. [134] This was later disallowed by regulators to keep UPI payments free for users and merchants. [134] To offset the resulting revenue loss, the government now provides direct subsidies to PSPs and TPAPs, particularly for low-value transactions and small merchants. These incentives are explicitly aimed at expanding UPI adoption in price-sensitive segments and geographies – especially tier III-VI cities – through products such as UPI Lite and UPI 123PAY. [135] In 2024, India's IT Ministry revealved that over Rs. 3600 crores had been spent on UPI incentives and promotions between 2021 and 2024. [134] In effect, a significant portion of the cost of operating UPI has been socialized through public funds, even as private firms continue to scale their user bases and associated revenue streams.

In parallel, many TPAPs have shifted toward data-driven ancillary revenue models. Firms such as PhonePe and Paytm monetize their position in the UPI ecosystem by selling value-added services to merchants and brands, including payment gateways, point-of-sale tools, digital lending, insurance, and targeted advertising. [136, 137] These services rely heavily on first-party transaction data – such as purchase behaviour, transaction frequency and value, location, and inferred life-stage indicators – to enable highly

[DRAFT — compiled at 2026-05-08 7:27; not for distribution]

granular targeting. For instance, Paytm advertises the following on their website: "Unlike third-party advertising platforms that rely on probabilistic targeting, Paytm's first-party transaction data enables precision targeting based on: [137] Actual purchase behaviour (not just browsing) Category preferences (food, beauty, electronics, etc.) Transaction frequency and value Geographic location Life stage indicators" As a result, while UPI transactions themselves are zero-priced at the point of use, the surrounding ecosystem has evolved into a profitable commercial layer built on behavioral and financial data generated through routine payment activity

4.6.5 Openness

The UPI ecosystem is closed and permissioned by design, with access limited to authorised participants rather than open to the public at large. The core UPI software is not open source, and its APIs are not open for unrestricted use. While UPI API specifications were initially published publicly, they were later withdrawn from NPCI's website, reducing transparency around the system's technical architecture. Today, UPI operates through closed APIs that are accessible only to approved actors, primarily banks acting as PSPs and their TPAPs.

Entry into the ecosystem is governed by a layered approval process. TPAPs may gain access to the UPI network only with NPCI's approval, and are required to meet specific compliance, security, financial stability, and technical standards set by NPCI. [138] PSPs face an additional regulatory threshold: they must first be licensed by the Reserve Bank of India as a payment aggregator or gateway, and only then may apply to NPCI to participate in the UPI system. [139] NPCI's control extends beyond onboarding to ongoing participation. It retains the authority to suspend or terminate UPI membership if participants fail to comply with UPI procedural guidelines or violate the rules of other NPCI-operated payment systems. Membership may also be withdrawn if a bank's mobile banking approval is cancelled by the RBI. [131] As a result, continued access to the UPI network is contingent not only on technical performance but also on sustained regulatory and contractual compliance.

At the application layer, NPCI has attempted to widen participation through the Bharat Interface for Money (BHIM) app, which is licensed to banks that do not operate their own UPI applications, allowing them to offer UPI services to customers without developing proprietary front-end infrastructure. [140]

In practice, UPI's openness is thus limited to interoperability among approved actors, rather than openness in the sense of open-source code, open APIs, or public contribution. While the system allows multiple approved actors to compete at the application and service layer, the underlying infrastructure remain centrally governed, with limited transparency, no open contribution model, and no pathway for participation outside NPCI's authorisation framework.

4.6.6 Coercion

Formally, UPI is a voluntary payment system, and there is no legal requirement for individuals to use it for everyday transactions. However, there are several regulatory mandates and broader policy choices that led to its near ubiquity in India's payment system. Amendments to the Finance Act, 2019 and the Income Tax Act, 1961 require businesses with annual turnover exceeding INR 50 crore to offer customers digital payment options, including UPI, RuPay debit cards, and UPI QR codes. [141] Although not a user obligation, this encouraged the rapid normalising of UPI as a default mode of payment.

Beyond formal legal requirements, state action and crisis-driven policy decisions have played a significant role in accelerating UPI adoption. The demonetisation exercise and the COVID-19-induced lockdowns temporarily constrained access to cash and physical banking services, making digital payment systems – UPI in particular – one of the few viable transaction channels for extended periods. [142] In parallel, the government actively promoted UPI through incentive schemes such as Lucky Grahak Yojana and DigiDhan Vyapar Yojana, which offered cash rewards to users and merchants for adopting digital payments. [143] While these measures did not mandate UPI use, they created strong economic and situational pressures that nudged individuals and businesses toward the system.

[DRAFT — compiled at 2026-05-08 7:27; not for distribution]

4.6.7 Data collection practices

UPI collects a combination of identity, financial, and transactional data at different stages of a user's interaction with the system.

During the UPI onboarding process, Payment Service Providers (PSPs) collect and store a defined set of personal, device-level, and financial identifiers that together establish a user's presence within the UPI ecosystem. At the point of registration, the system collects the user's mobile number, which is verified through an automated, encrypted SMS sent from the user's SIM card. [144] This process results in a strong binding between the mobile number and the physical device, enabling the PSP to record both identifiers and link them persistently. The PSP application (including delegated third party apps) also captures and stores device identifiers, which are used to enforce device-level authentication and prevent account access from unregistered hardware. [131] Users are required to create a UPI ID (Virtual Payment Address), which becomes a persistent identifier for initiating and receiving payments across the network. The customer's name, as entered or displayed within the PSP application, is also retained. [131]

When a user links a bank account, the issuing bank shares masked bank account details, including the account number and IFSC code, associated with the verified mobile number. These details are transmitted via the UPI system to the PSP and stored in the PSP's database, where they are mapped to the user's mobile number, UPI ID, and device identifier. [131] As a result, the PSP maintains a consolidated dataset that links identity (mobile number and name), financial information (bank account and IFSC), and device-level data, forming the basis for all subsequent UPI transactions. Aadhaar-based onboarding is also available, in which case Aadhaar credentials are used as part of the registration process. Know-Your-Customer (KYC) information is not collected independently by UPI itself, but is sourced from the linked bank account or from Aadhaar data used during sign-up. All financial transactions are governed by mandatory two-factor authentication: the first factor is validated by the PSP, while the second factor is validated by the issuing bank. Where biometric authentication is used, fingerprints or iris data are verified by UIDAI as a trusted third party on behalf of the issuing bank. [131]

Through use of the service, UPI generates and processes detailed transactional data. This includes the user's Virtual Payment Address (VPA), transaction amounts, timestamps, transaction type, merchant codes, and information about the counterparty to the transaction. Bank account details are necessarily involved in the backend for debits and credits. Mobile numbers also form a significant data point: in 2021, NPCI permitted PSPs to use a user's mobile number as a numeric UPI ID in place of a VPA, which led to instances where payers' phone numbers were shared with merchants and banks. [145] In response, NPCI issued an addendum in March 2025 requiring explicit user consent and opt-in for this feature. [146] Location data may also be collected, although this has since been made optional.

Beyond core payment functionality, PSPs and TPAPs often collect additional data when offering ancillary services such as loans, fraud detection, credit scoring, or insurance. [136, 137] Transaction histories, spending patterns, location data, and inferred demographic information are frequently repurposed for targeted advertising and personalised service offerings. As several privacy experts have noted, this data-centric design – characterised by extensive collection and sharing of user data across multiple participants in a single transaction – is integral to UPI's architecture. [20] It is also one of the reasons the system can operate without charging direct transaction fees, shifting the economic model toward monetisation of data and downstream services rather than payment processing itself. This data collection/use is not governed through the UPI framework, and will be found in the individual PSP/TPAP's privacy policies.

4.6.8 Data sharing and linking with other databases

UPI adopts a distributed data storage model, in which user and transaction data is available across multiple actors involved in a payment. Depending on the stage of the transaction, data may be stored by the payer-side PSP and TPAP, the payee-side PSP and TPAP, the remitter bank, and the beneficiary bank. Only NPCI holds the complete dataset for a transaction and different components of user and payment data are retained at various points in the ecosystem, based on role and function.

Under the 2019 UPI Procedural Guidelines, customer data is broadly defined to include personal and transactional information such as the customer's name, mobile number, address, email ID, gender, and (where provided) location details, along with device-level identifiers like app ID and IMEI number. [131]Transaction-related data – such as the UPI ID, transaction reference number (RRN), transaction ID, timestamps, ben-

[DRAFT — compiled at 2026-05-08 7:27; not for distribution]

eficiary UPI ID, beneficiary account number, and the beneficiary's core banking system identifier – is also included. All such UPI transaction data is required to be stored by app providers in encrypted form. This dataset is used not only for completing a transaction but also for enabling subsequent transactions and dispute resolution. [131]

A narrower category of payment-sensitive data, including bank account numbers and authentication-related information such as device fingerprinting, is subject to stricter storage controls. This data may be stored only within PSP bank systems, and even then with limitations. Certain elements, such as full debit card numbers, expiry dates, UPI PINs, and issuer OTPs, are explicitly prohibited from being stored. Where account information is displayed to users within an app, it must be shown only in masked form. [131]

These storage practices are overlaid by the Reserve Bank of India's data localisation mandate for payment systems. Under the RBI's April 2018 circular on the Storage of Payment System Data, all payment system operators are required to ensure that the entire end-to-end transaction data relating to payments is stored only in systems located in India. [133] While limited foreign storage is permitted for the offshore leg of a transaction where necessary, the directive emphasises the need for unfettered supervisory access by Indian regulators to data held by system providers, intermediaries, and third-party vendors across the payment ecosystem. [133]

4.6.9 Data security and privacy

The data security losses in the UPI ecosystem spans issues like monetary theft, from both individuals and institutions, denial of service from critical payments infrastructure and disruption of country-level payment systems and the services that have come to rely on it. Responsibility for data security within the UPI ecosystem is accorded depending on where the data resides at any given point in the transaction lifecycle. Under NPCI's procedural guidelines, NPCI assumes responsibility for the security and integrity of data once it enters and remains within the NPCI network. When data is held or processed outside the NPCI network – whether by PSPs, banks, TPAPs, or other intermediaries – security and authenticity obligations shift to the entity in possession of that data. [131] This results in a fragmented liability model, where responsibility is distributed rather than centrally enforced. PSP banks retain primary responsibility for safeguarding user data even where parts of the technical stack are outsourced. The guidelines make clear that security and data integrity obligations do not transfer to third-party technology vendors, and that PSPs and banks are expected to conduct due diligence when engaging external service providers who may handle sensitive customer or transaction data. [131]

Under CERT-In Directions issued in 2022, cybersecurity incidents, including data breaches, must be reported to CERT-In within six hours of detection. [147] Banks are also required to notify the RBI. However, there is no corresponding obligation to notify affected users. While future requirements under the Digital Personal Data Protection Act may introduce user notification obligations, these are not yet in force.

Concerns around the effectiveness of this security model are underscored by past incidents. A government audit completed in early 2019 identified more than forty cybersecurity vulnerabilities across NPCI-operated payment infrastructure, including instances of sensitive user information being stored in plain text. [148] Several of these vulnerabilities were classified as critical or high-risk. NPCI has since stated that the identified issues were addressed, but the episode highlights the opacity of security oversight within the UPI ecosystem and the absence of routine public disclosure around vulnerabilities or remedial actions.

UPI does not operate a public vulnerability disclosure program or bug bounty mechanism and its source code, specifications and APIs are not available to the general public for scrutiny. While security by obscurity may be a viable model for lesser known software systems, it does not benefit a foundational payment system that operates at nation scale.

5 Overall Analysis

5.1 Introduction and ownership

Across the DPIs we studied, the dominant model is the "public-purpose private entity". Three of the six DPIs (UPI, Bharat BillPay, and FASTag's payment layer) are operated directly by NPCI or its subsidiaries – a Section 8 non-profit company owned by a consortium of 65 shareholder banks. Only Aadhaar eKYC

[DRAFT — compiled at 2026-05-08 7:27; not for distribution]

(operated by UIDAI, a statutory authority) and DigiLocker (operated by NeGD under the Digital India Corporation, a government Section 8 company) are owned entirely by the government. The consortium model is a deliberate design choice for public digital infrastructure in India: a 2011 advisory committee, chaired by Nandan Nilekani, recomended vesting DPI ownership in industry-led non-profit companies rather than government departments to enable faster procurement and cut through some of the bureaucratic red tape typical to government projects. [149] The model was successful in many ways, particularly in building and scaling infrastructure quickly. However, it has created a significant accountability gap. NPCI is not subject to the Right to Information Act (RTI) , and has actively disputed its status as 'state' under Article 12 of the Constitution before both the Central Information Commission and the Madras High Court, arguing that it is a private company and not a public authority. [150] There has been no definitive ruling on this as of yet. As a result, the entity processing over 80% of India's digital payment volumes in 2025 has no statutory obligation to disclose failure rates, fraud statistics, or dispute resolution outcomes to the public. [151] UPI has suffered several major outages and failures, but these have only occasionally been acknowledged by NPCI, with no other information about the cause publicly disclosed. [152] Thus, even with NPCI receiving over INR 8,000 crore in public subsidies between 2021 and 2025 for UPI and RuPay promotion, and having 51% of its equity being held by public sector banks, citizens cannot use RTI to access information about how these public funds are spent or how NPCI's decisions are made. [150]

A related but distinct structural issue we observed is where the government body that regulates a DPI ecosystem is also the sole operator within it. This is the case for DigiLocker. The 2016 Digital Locker Rules had originally envisioned a federated ecosystem of licensed Digital Locker Service Providers (DLSPs) operating under a common regulatory framework. However, when no DLSPs emerged, MeitY simultaneously became the rule-setter for standards, data protection, and privacy, and the product owner that designs, manages, and promotes DigiLocker's growth. [62]

5.2 Development and deployment

DigiLocker represents the only example in our study of a DPI that remains entirely owned and operated by public bodies. MeitY, through the National e-Governance Division, built the platform in-house and continues to serve in a dual capacity as both operator and regulator – a consequence of the original federated ecosystem of licensed Digital Locker Service Providers never materialising.

The more common thread across other DPIs is the limited role of the state in setting "rules of the road", while private companies increasingly lead the development, deployment, operations and maintenance of the actual systems. The NPCI, established at the initiative of the RBI and the Indian Banks' Association, remains a key actor in multiple DPIs – operating FASTag's centralised settlement system; building Bharat Connect's transaction processing platform; and building and owning UPI's central infrastructure. Notably, the NPCI is a privately-incorporated and bank-owned entity. NPCI itself has argued that it is *not* part of the "state" for the purposes of Article 12 of the Constitution of India. [153]

The Account Aggregator is another example in which the state sets regulatory parameters but operates little to no actual infrastructure. The RBI's Master Directions establish the licensing requirements and governance framework, but private companies that meet these requirements register and operate as AAs independently. Notably, an industry alliance (Sahamati) has assumed a significant coordinating role, publishing resources, streamlining certification processes, and promoting ecosystem adoption. This private-sector leadership in what might otherwise be regulatory functions may soon receive formal recognition through the RBI's recent framework for self-regulatory organisations in the AA ecosystem.

Aadhaar eKYC occupies a hybrid position: while UIDAI owns and operates the central identity infrastructure and the CIDR, the service delivery layer is populated by private Authentication User Agencies, KYC User Agencies, and Authentication Service Agencies operating under UIDAI's access conditions.

Overall, our findings highlight the predominance of private companies in the development and practical ownership of DPIs in India. This is not withstanding that large portions of actual operations are delegated to other private companies. For FASTag, banks distribute tags, acquiring banks process transactions with toll operators, and private technology vendors operationalise toll plazas For BharatConnect, NBBL handles settlement, technology providers connect through the NBBL Developer Program to deliver services. For UPI, NPCI governs the network and provides core switching infrastructure, Payment Service Providers and Third-Party Application Providers drive customer acquisition and deliver user-facing services.

[DRAFT — compiled at 2026-05-08 7:27; not for distribution]

5.3 Governance

The governance architectures of India's DPIs reveal a consistent structural pattern: regulatory authority is concentrated in central state bodies, while operational governance is delegated through layered frameworks of rules, guidelines, and bilateral agreements. However, the specific configuration of this delegation, and the mechanisms for accountability, transparency, and stakeholder participation vary considerably across systems.

In all six DPIs, ultimate regulatory authority rests with a central government body: the RBI for UPI, Account Aggregator, and Bharat Connect; UIDAI for Aadhaar eKYC; MeitY for DigiLocker; and MoRTH/NHAI for FASTag. These bodies retain powers of authorisation and inspection. However, day-to-day operational governance is typically delegated to entities that may be private or public: NPCI for UPI, FASTag, and Bharat Connect; IHMCL for FASTag policy enforcement; and the DigiLocker Authority for DigiLocker.

Across the DPIs studied, compliance gets scattered across entities and documents of varying legal status. We can see that enforcement mechanisms are generally strongest where the regulator retains direct power. The RBI may cancel an AA's Certificate of Registration for non-compliance, and NPCI may suspend or terminate membership from the NETC or UPI systems. FASTag is an exception, where the rules do no specify how a non-compliant entity may be removed from the system. However, enforcement against vendors and and intermediaries sometimes remains unclear.

The transparency and accountability of such systems the public is hampered in concrete ways when key functions are delegated to private or semi-private bodies. For example, the public can't exercise their Right to Information (RTI) and seek details from participating entities if they are not government-controlled or created. As noted before, this is documented well for NPCI's case, which has argued that it not a public authority, has refused to respond to RTIs. [153]

While formal mechanisms for stakeholder deliberation exist in some DPIs, they are limited in scope and authority. Bharat Connect's Steering Committee and UPI's Steering Committee bring together representatives from participating institutions in an advisory capacity. No DPI examined has an independent oversight board or parliamentary committee with specific supervisory powers. Most pertinently, public participation and input is nearly absent for all DPIs.: public consultation before a launch was documented only for Account Aggregator, while the remaining systems were introduced primarily through directives without public engagement.

5.4 Economic and business models

Across the DPIs we examined, no single economic model predominates. Instead, a spectrum emerges: from publicly funded utilities to hybrid arrangements to explicitly commercial platforms. DPIs vary significantly in how costs, revenues, and risks are distributed among the state, regulated intermediaries, and private actors.

At the public-good end of the spectrum, DigiLocker and UIDAI's eKYC infrastructure are sustained primarily through government appropriations. UIDAI received Grants-in-Aid from MeitY, recovering the shortfall from its own service receipts [41]. DigiLocker's core application is similarly grant-funded and free to end-users, though the rules permit fee-charging for premium features.

FASTag and UPI occupy a middle position, characterised by no directly-visible pricing for the service at the point of use *per se*. Instead, the government transfers funds to private intermediaries. In FASTag, each toll transaction triggers fixed programme-management disbursements to the acquirer bank, issuer bank, NPCI, and IHMCL [28]. UPI has similarly shifted the revenue burden away from merchants: between 2021 and 2024, the government disbursed over ₹3,600 crore in UPI incentives and promotions to offset resulting losses [114]. In both cases the infrastructure is presented as a public utility while a considerable portion of its operating cost is borne by public funds channeled to private financial institutions.

Bharat Connect and the Account Aggregator framework represent the most commercially developed end of the spectrum. NPCI Bharat BillPay Limited, despite being a subsidiary of NPCI, is an explicitly for-profit entity. Private Operating Units (e.g., PayTM, PhonePe, and Google Pay) generate additional revenue through transaction fees, financial product cross-selling, and merchant commissions [109]. Srikanth et al. document a further layer of monetisation: bill-payment behavioural data collected on the platform is used to construct consumer credit profiles, constituting commercial exploitation of data generated incidental to a nominally public infrastructure service [116]. The Account Aggregator ecosystem exhibits an analogous

[DRAFT — compiled at 2026-05-08 7:27; not for distribution]

dynamic. Virtually all licensed AAs are private for-profit companies and charge a per-transaction fee while being prohibited by RBI from diversifying into any ancillary business [87, 83]. Growth in the ecosystem has been driven overwhelmingly by unsecured consumer lending, which suggests that the framework, though cast as a financial-inclusion tool, primarily serves the credit-origination interests of private lenders [89, 88].

Our findings surface a structural pattern: DPIs in India are rarely funded and operated as unambiguous public goods. Even where access is formally free and nominal governance rests with a government body or a non-profit entity, the surrounding ecosystem typically incorporates for-profit intermediaries whose incentives are shaped by transaction volumes, data accumulation, and cross-selling opportunities. State subsidies and regulatory mandates frequently underwrite private revenue streams rather than eliminate them, raising questions about whether the public-infrastructure framing of DPI accurately describes the distribution of benefits and risk.

5.5 Openness

Across the DPIs we examined, openness emerges as a consistently aspirational rather than operational characteristic. While international frameworks advocate for open-by-default design, reusable standards, and community participation, India's DPI stack reveals a systematic preference for permissioned, controlled ecosystems over genuinely open infrastructure [18].

Source code availability is the narrowest dimension of openness across the corpus. FASTag is fully closed, with no public components and participation restricted to entities empanelled by NPCI under agreements with IHCML [27]. UPI's core software is similarly proprietary: API specifications that were once publicly available were subsequently withdrawn, reducing rather than expanding technical transparency over time. Bharat Connect has released a single open-source component, but no element of the core BBPS transaction-processing infrastructure is publicly accessible [110]. DigiLocker and Aadhaar eKYC publish technical specifications and API documentation, yet neither permits unrestricted use or adaptation. Access in both cases is gated by formal onboarding and legal agreements [39, 154]. Account Aggregator is the partial exception: because it is a decentralised framework rather than a single service, there is no central codebase and ReBIT's publicly available API specifications have enabled an ecosystem of open-source libraries and sandbox environments maintained by private participants (e.g., Setu, Finvu) [80].

API access follows a similar pattern: every system examined confines programmatic integration to approved actors. Bharat Connect requires NPCI certification and operates over a managed network [101]. UPI extends API access only to RBI-licensed payment aggregators and NPCI-approved TPAPs. Aadhaar eKYC is available solely to UIDAI-designated KUAs. The effect is that interoperability, which is often cited as a defining benefit of DPI, operates within a closed circle of regulated incumbents rather than as a genuinely open technical commons.

Governance participation is equally constrained. With the partial exception of the Account Aggregator ecosystem, no system provides public issue trackers, open mailing lists, or community contribution mechanisms [84]. Bharat Connect's formal Steering Committee constitutes the only governance forum for the system, yet its proceedings are not public [112]. Operational transparency is likewise absent: no DPI maintains a public uptime dashboard or real-time status page, despite Bharat Connect's own documented 99.5% availability requirement [101].

Our findings suggest that openness in India's DPI stack is deployed selectively to attract ecosystem participation and signal public interest intent, while substantive control over code, specifications, and governance remains concentrated in NPCI and the relevant sectoral regulators. This architecture may serve legitimate security and stability objectives, but it also limits independent auditability, forecloses community-led innovation, and creates structural barriers to entry that disproportionately favour large incumbents. DPI design and evaluation frameworks should distinguish clearly between interoperability among approved actors and genuine openness as a public-interest property.

5.6 Coercion

The DPIs examined range from formally voluntary to explicitly mandatory, but there exist extra-legal pressures even when DPIs are not mandated by law.

[DRAFT — compiled at 2026-05-08 7:27; not for distribution]

FASTag represents the clearest case of a legal mandate: amendments to the Motor Vehicles Act made its use mandatory for toll payment in January 2021, with no legally permissible alternative.

Aadhaar eKYC exemplifies a form of coercion regardless of no direct legal mandate. While officially voluntary, Aadhaar authentication has become a prerequisite for welfare entitlements that vulnerable populations cannot forgo – Direct Benefit Transfers, PDS rations, and LPG subsidies all require Aadhaar linkage. In these contexts, "consent" functions less as choice and more as condition of access. DigiLocker occupies a somehwat similar position: individual use is formally voluntary, but the system is mandatory for government departments and educational institutions, with instances of *de facto* mandates emerging without formal legal change.

Often, structural and situational pressures have guided the expansive reach of DPIs like UPI and Bharat Connect. UPI remains formally voluntary, but constraints on cash during demonetisation and COVID-19 created powerful pressures toward adoption. Bharat Connect similarly mandates participation at the infrastructure level, with all bill-payment intermediaries required to route through BBPS.

Even where consent mechanisms exist, implementation gaps persist. Bharat Connect Operating Units have retrieved consumer data without transaction-specific consent.

Account Aggregator stands as the strongest consent-centric design among the DPIs studied, with explicit consent requirements embedded in regulation – but predatory practices and malicious compliance by companies can often undercut the spirit of such consent.

5.7 Data collection, sharing and privacy

The DPIs we examined collect and operate on large amounts of private information, including user identifiers such as name, mobile number and biometric captures, cross-service identifiers like PAN Card number, Aadhaar number and device ID, demographic details, sensitive documents and credentials, and financial information. Regular usage of DPIs also generates detailed behavioural records about users, that can reveal where they travel, what they purchase, and which businesses, institutions and services they interact with.

Our analysis of the information architectures of DPIs revealed that various entities playing different roles within respective DPIs have differing levels of visibility into user data and face different regulatory constraints on what they can do with it. For example, an Authentication User Agency (AUA) performing Aadhaar authentication or a Third-Party Application Provider (TPAP) facilitating UPI payments will only see data belonging to the subset of users that they serve. AUAs are barred from using or retaining demographic data and only maintain operational logs, whereas TPAPs are allowed access to the financial transactions of their users and are even permitted to monetise this data in aggregate form. The DPIs in our case studies (with the exception of Account Aggregator and DigiLocker) also contained a centralised entity that coordinates the service and has complete visibility into all of the data that flows through the system. Examples of this include, the Central Identities Data Repository (CIDR) in Aadhaar, the National Payments Corporation of India (NPCI) in UPI and BharatConnect, and the National Electronic Toll Collection (NETC) Mapper in FASTag.

Another defining characteristic of data collection practices of DPIs in India is the prevalence of linking disparate databases. Linking (or seeding) occurs when a unique user identifier, such as an Aadhaar number or mobile number, is present in disparate databases and can be used to correlate user activity across them. For example, a mobile number that is used to sign up for UPI, Aadhaar, DigiLocker and FASTag, can be used to correlate user activity across these disparate systems. Indian residents are required to link their Aadhaar number with their Tax ID (PAN Card) and there is also an initiative to link it to Voter IDs. DigiLocker encourages document issuers to verify and link documents added to DigiLocker to users' Aadhaar details, bringing data that has previously existed in silos, such as driving licenses, educational degrees and caste certificates, into the ambit of DPI-enabled user activity correlation.

The scale and universality of DPIs means that the private data generated through their use and linkage is qualitatively different from the analog and digital processes they seek to replace — it is more comprehensive, more reliably identified, and harder for individuals to opt out of. As DPIs permeate into more aspects of everyday life — such as payments, identification, healthcare, welfare distribution, e-commerce and travel — the behavioural records generated by these services can be misused for targeted and mass surveillance. It can be used to infer demographic information, political leanings, consumption patterns, health conditions, travel history and other behavioural traits of not just individuals, but entire populations.

[DRAFT — compiled at 2026-05-08 7:27; not for distribution]

For example, an actor with access to NPCI's UPI transaction records, the NETC Mapper's FASTag toll data, and the CIDR's Aadhaar authentication logs could build continuously updated socioeconomic profiles of the electorate. Spending patterns from UPI logs could be used to infer political leanings and consumption habits; FASTag records could reveal attendance at religious sites, political gatherings, or protest locations; and demographic attributes from Aadhaar could be layered on top.

The regulatory framework has actively permitted these risks rather than constraining them [155]. Private actors operating UPI payment apps are authorised to record users' financial transactions and monetise derived data products. The Supreme Court's 2018 restrictions on private use of Aadhaar have since been narrowed by legislative amendment [43]. Government access to DPI data operates under broad statutory exemptions with no meaningful independent oversight mechanism [156, 157]. Our analysis of policies that govern DPIs also revealed that there are no checks in place for extending the use of DPI infrastructure and data for purposes other than what was initially stated. For example, the FASTag system was integrated with the Goods and Services Tax (GST) department [34] even though there was no provision to do so in its governance policies. Crucially, there is also nothing that prevents or governs such additional use. Given that most DPIs contain centralised data stores with API-enabled access, the architecture for population-level profiling already exists and is ripe for abuse. Reports indicate that data from Aadhaar and FASTag is already being used for this purpose [158].

These privacy issues are not unique to DPIs, equivalent commercial services suffer similar limitations. Commercial payment processors hold similar datasets to NPCI and online advertising companies create detailed behavioural records by following users across the internet. However, DPIs exacerbate these issues by associating behaviour with government-issued IDs, linking disparate datasets that previously only existed in silos, creating centralised points of data access, and pushing for nationwide adoption, all while creating a false sense of safety by positioning themselves as public-interest technologies.

5.8 Data security

Our analysis of DPIs revealed the presence of formal security controls, particularly for the financial DPIs (UPI, Bharat Connect and Account Aggregator) that fall under the regulatory ambit of the RBI. These include security certifications, periodic audits, incident reporting requirements and limiting participation to vetted operators. We found that the security processes fell short of software industry standards in two ways: (1) Lack of responsible disclosure policies and bug bounty programs: most DPIs we examined did not have policies in place for security researchers to responsibly disclose security vulnerabilities, nor did they incentivise security research through bug bounty programs. On the contrary, researchers and journalists reporting cybersecurity issues in DPIs have faced harassment and legal threats [159, 160, 161]. (2) Security through obscurity: Several DPI operators have hidden APIs, specifications, source code and architectural design documents from public view. While obscuring technical details and secrecy may be a viable strategy for lesser known software, widely used infrastructure can benefit from sustained adversarial analysis by the research community.

When faced with security vulnerabilities and data breaches, DPIs defined their security perimeter narrowly. The security boundary was set to be at the core infrastructure, while responsibility for breaches occurring through third-party integrators and components was denied. In the Aadhaar ecosystem, for example, UIDAI's security posture centres on the CIDR, yet data exposures have occurred through poorly secured AUAs and state government integrators rather than through UIDAI's own systems [53, 54, 55]. The same pattern is visible in UPI. In 2020, over seven million records belonging to BHIM users, including Aadhaar scans, PAN cards, caste certificates, and UPI handles, were exposed through cloud storage belonging to a government-partnered agency running a merchant onboarding campaign for the app [162]. NPCI denied any breach of the BHIM app itself, a technically accurate but misleading response, as the data had leaked through a third-party campaign that sought to expand BHIM's user base. Defining a breach as "access to the central repository" while ignoring the broader ecosystem understates the actual attack surface and allows operators to report clean security records while sensitive data leaks through the periphery.

The Aadhaar identity system has, in particular, made poor security choices. It relies on weak authentication factors, like biometrics and SMS-based OTPs to secure critical demographic and biometric information of over a billion users. Biometrics like fingerprints and iris scans are publicly visible identifiers and cannot be changed in case of a breach. In 2023, the Indian Cyber Crime Coordination Centre issued an alert that

[DRAFT — compiled at 2026-05-08 7:27; not for distribution]

criminals were copying fingerprints from state land registry websites to conduct fraudulent AePS withdrawals [163, 164], following which liveness checks were implemented [165]. SMS-based OTPs are susceptible to SIM swap attacks, where telecom operators are fraudulently convinced to transfer mobile number ownership, and fail when expired mobile numbers are reassigned to new users [166].

6 Conclusion

Across all dimensions – openness, governance, transparency, security and privacy – DPIs in India fall short not only of the aspirational principles of DPI set by academics and civil society, but also of the claims of the Indian government itself.

Notably, in no DPI we studied, was there any forum or avenue for public participation. Only in the case of Account Aggregators, there was initial public consultation – but no ensuing similar practice in the next ten years wherein the AA system and regulations evolved considerably. As our analysis of the ownership, development and deployment of Indian DPIs shows, many key functions of DPIs (and sometimes even regulation) is delegated to private companies that are impervious to public scrutiny. Overall, there is hardly any public control or public say over digital *public* infrastructure.

The Government's claims that Indian DPIs are "open" also do not stand up to empirical scrutiny. FASTag is an example of a system that is fully closed-source, while other DPI implementations predominantly have proprietary code unavailable to the public. In cases where API specifications are public, the API is closed to a set of entities – even of functionalities that could be made open to the public. For UPI, there is even a regression in openness, with no up-to-date API specifications made available to to the public. There are sparse repositories of open source code, but the core infrastructure remains a black box to the vast population that engages daily with DPIs.

When it comes to privacy, these DPIs do not just reproduce the risks of equivalent commercial services, but compound them by binding behavioural records to government-issued identifiers, linking activity across services that previously existed in silos, and concentrating data in centralised repositories accessible to state actors under broad statutory exemptions. On the security front, Indian DPIs have deployed authentication mechanisms with documented weaknesses, defined their security perimeter narrowly to exclude third-party integrators through whom most real-world breaches occur, and forgone the adversarial scrutiny that open specifications would invite.

Digital Public Infrastructure may hold some promise for reimagining service delivery and governance in the digital age. Yet as India's experience shows, the form that DPI takes is deeply political. Without clarity on principles of ownership, participation, and accountability, DPI risks becoming a vehicle for privatizing public functions under the guise of technological modernization. As the concept continues to spread globally, critical scrutiny is essential to ensure that DPI serves the public interest rather than undermines it.

[DRAFT — compiled at 2026-05-08 7:27; not for distribution]

References

[1] Julia Clark, Georgina Marin, Oya Pinar Ardic Alper, and Guillermo Alfonso Galicia Rabadan. Digital public infrastructure and development: A World Bank Group approach. Digital Transformation White Paper Volume 1, The World Bank, Washington, DC, March 2025. Accessed: 2026-03-31.

[2] Press Information Bureau, Ministry of Electronics and Information Technology, Government of India. India has signed MoU/agreements with 23 countries for cooperation on Digital Public Infrastructure (DPI), February 2026. Release ID: 2224505. Accessed: 2026-03-31.

[3] Mila T Samdub. "Digital Public Infrastructure" at a turning point: From definitions to motivations. Technical report, Open Future, February 2025. Accessed: 2026-03-17.

[4] Ethan Zuckerman. What is digital public infrastructure? `https://www.journalismliberty.org/publications/what-is-digital-public-infrastructure`, November 2020. Accessed: 2026-03-17.

[5] Mila T Samdub and Chand Rajendra-Nicolucci. What is digital public infrastructure? towards more specificity. `https://www.techpolicy.press/what-is-digital-public-infrastructure-towards-more-specificity`, November 2024. Accessed: 2026-03-17.

[6] Amitabh Kant and Nandan Nilekani. Report of India's G20 task force on digital public infrastructure. Task force report, India's G20 Task Force on Digital Public Infrastructure for Economic Transformation, Financial Inclusion and Development, Department of Economic Affairs, Ministry of Finance, Government of India, July 2024. Final report released during India's G20 Presidency. Co-Chairs: Amitabh Kant (G20 Sherpa of India) and Nandan Nilekani (Co-founder of Infosys, Founding Chairman of UIDAI).

[7] David Eaves and Jordan Sandman. What is digital public infrastructure? `https://medium.com/iipp-blog/what-is-digital-public-infrastructure-6fbfa74f2f8c`, April 2023. Accessed: 2026-03-17.

[8] Centre for Digital Public Infrastructure. DPI tech architecture principles. `https://docs.cdpi.dev/the-dpi-wiki/dpi-tech-architecture-principles`, 2023. Accessed: 2026-03-17.

[9] G20 India. G20 digital economy ministers' meeting outcome document and chair's summary. G20 Official Document, August 2023.

[10] G7 Digital and Tech Ministers. G7 ministerial declaration. `https://www.gov.uk/government/publications/g7-ministerial-declaration-cernobbio-italy-15-october-2024/g7-ministerial-declaration-15-october-2024`, October 2024. Cernobbio-Como, Italy. Accessed: 2026-03-17.

[11] OECD. Digital public infrastructure for digital governments. Technical Report 68, OECD Publishing, Paris, December 2024.

[12] David Eaves and Krisstina Rao. Digital public infrastructure: A framework for conceptualisation and measurement. Technical Report IIPP WP 2025-01, UCL Institute for Innovation and Public Purpose, London, January 2025. Accessed: 2026-03-17.

[13] Anita Gurumurthy, Nandini Chami, Sadhana Sanjay, Rudraksh Lakra, and Eshani Vaidya. Recovering the 'Public' in India's digital public infrastructure strategy. Technical report, IT for Change, January 2025. Accessed: 2026-03-17.

[14] Mariana Mazzucato, David Eaves, and Beatriz Vasconcellos. Digital public infrastructure and public value: What is 'public' about DPI? Working paper wp 2024-05, UCL Institute for Innovation and Public Purpose (IIPP), March 2024.

[15] Central Bank of Brazil. Pix management report: Conception and first years of operation, 2020–2022. Technical report, Banco Central do Brasil, 2023.

[DRAFT — compiled at 2026-05-08 7:27; not for distribution]

[16] World Bank. Fast payments toolkit: Case study — Thailand PromptPay. Technical report, World Bank, 2021. World Bank Fast Payments Toolkit.

[17] David Eaves, Diane Coyle, Beatriz Vasconcellos, and Sumedha Deshmukh. The economics of shared digital infrastructures: A framework for assessing societal value. Iipp policy report 2025/02, UCL Institute for Innovation and Public Purpose and Bennett Institute for Public Policy, Cambridge University, March 2025.

[18] United Nations Office of Information and Communications Technology. The OSI first to endorse United Nations open source principles. https://unite.un.org/en/news/osi-first-endorse-united-nations-open-source-principles, February 2025. News release. Accessed: 2026-03-17.

[19] Press Information Bureau. India's digital public infrastructure: Setting a global benchmark for population-scale DPI. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2235812, March 2026. PRID 2235812. PIB Delhi.

[20] Umang Poddar. Are your UPI payments farming your personal data without your consent? *Scroll.in*, March 2023.

[21] National Payments Corporation of India. About FASTag – National Electronic Toll Collection. https://www.netc.org.in/about-fastag#trnflow. Accessed: 2026-03-17.

[22] Press Information Bureau. Electronic toll management system. http://pib.nic.in/newsite/PrintRelease.aspx?relid=154486, 2016. Government of India, Ministry of Road Transport & Highways. Accessed: 2016-12-20. Archived at https://web.archive.org/web/20161220145515/http://pib.nic.in/newsite/PrintRelease.aspx?relid=154486.

[23] Indian Highways Management Company Limited. About us – IHMCL. https://ihmcl.co.in/about-us/. Accessed: 2026-03-17.

[24] Indian Highways Management Company Limited. Annual report 2023–24. Technical report, Indian Highways Management Company Limited, 2024. Accessed: 2026-03-17.

[25] The Wire Staff. FASTag: Will datafication of India's tolls boost highway development? *The Wire*, December 2019.

[26] National Payments Corporation of India. Procedural guidelines: National electronic toll collection network (NETC network). Version 1.9, National Payments Corporation of India, 2022. Accessed: 2026-03-17.

[27] National Payments Corporation of India and Indian Highways Management Company Limited. NETC interface control document (ICD) manual. Version 2.5, National Payments Corporation of India, 2020. Accessed: 2026-03-17.

[28] Lok Sabha. Unstarred question no. 1529: Issue of FASTag and revenue sharing with states. https://sansad.in/getFile/annex/260/AU1529.pdf?source=pqars. 260th Session of Lok Sabha, Parliament of India. Accessed: 2026-03-17.

[29] Press Information Bureau. MoRTH issues notification for promotion of digital and IT based payment of fees through FASTag; all 4 wheel vehicles required to have FASTags from 1st January 2021. https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=1671049, November 2020. Government of India, Ministry of Road Transport & Highways. Release ID: 1671049.

[30] Ministry of Road Transport and Highways, Government of India. Reply to Rajya Sabha unstarred question no. 1440 on toll charges, February 2026. Rajya Sabha, Session 270. Accessed: 2026-04-27.

[31] National Highways Authority of India. National highways fee rules, 2026 amended to strengthen toll compliance and digital enforcement, March 2026. Press Release. Accessed: 2026-04-27.

[DRAFT — compiled at 2026-05-08 7:27; not for distribution]

[32] Indian Highways Management Company Limited. Frequently asked questions on FASTag – version 1. Technical report, Indian Highways Management Company Limited. Published by NHAI. Accessed: 2026-03-17.

[33] New Indian Express. Beware! vehicles sans insurance can now be e-detected at toll gates. *The New Indian Express*, January 2025.

[34] Advait Palepu. How the NPCI's FASTag system is being integrated with E-Way bill system. *MediaNama*, May 2021.

[35] Soumyarendra Barik. FASTag details to be 'captured' upon vehicle registration, fitness certificate issuance: MoRTH. *MediaNama*, July 2020.

[36] Cyble Research Labs. Toll plaza data exposure. *Cyble Blog*, December 2021.

[37] Dark Web Informer. A threat actor has allegedly leaked the ICICI bank etoll/FASTag database. *Dark Web Informer*, August 2024.

[38] Archisman Bhattacharjee. Setu-ing the standard: NPCI's new path to Aadhaar e-KYC. *Vinod Kothari Consultants*, August 2025.

[39] Unique Identification Authority of India. Aadhaar e-KYC API specification – version 2.5. Technical report, Unique Identification Authority of India, Government of India, August 2019. Accessed: 2026-03-17.

[40] Reserve Bank of India. Master direction – know your customer (KYC) direction, 2016. `https://www.rbi.org.in/CommonPerson/english/scripts/notification.aspx?id=2607`, 2016. Updated as on August 14, 2025. Accessed: 2026-03-17.

[41] Unique Identification Authority of India. UIDAI annual report 2023–24. Technical report, Unique Identification Authority of India, Government of India, 2024. Accessed: 2026-03-17.

[42] Unique Identification Authority of India. Authentication requesting agency. `https://uidai.gov.in/en/ecosystem/authentication-ecosystem/authentication-requesting-agency.html`. Government of India. Accessed: 2026-03-17.

[43] MediaNama. Private companies now free to use Aadhaar for authentication. *MediaNama*, February 2025.

[44] Unique Identification Authority of India. The Aadhaar (payment of fees for performance of authentication) regulations, 2023. `https://uidai.gov.in/images/5_The_Aadhaar_Payment_of_Fees_for_Performance_of_Authentication_Regulations_2023.pdf`, 2023. Notification No. HQ-13073/1/2020-AUTH.II(E), dated 29.09.2023. Published in the Gazette of India, Part III, Section 4. Updated as on 23.10.2023.

[45] Unique Identification Authority of India. Circular no. 04 of 2023: Revising license fee for AUA/KUA. `https://uidai.gov.in/images/resource/Circular_No_04_of_2023_revising_License_fee_AUA_KUA_05042023.pdf`, April 2023. Accessed: 2026-03-17.

[46] Unique Identification Authority of India. AUA/KUA onboarding process, application form and audit compliance checklists. Technical report, Unique Identification Authority of India, Government of India. Accessed: 2026-03-17.

[47] Times of India. Direct benefit transfers: Govt makes Aadhaar authentication must for all centrally sponsored schemes, aim to ensure transparency. *The Times of India*, 2025.

[48] Rajasthan Jan Aadhaar Authority. Jan Aadhaar e-KYC. `https://janaadhaar.rajasthan.gov.in/content/raj/janaadhaar/en/home-page_detail/jan-aadhaar-e-kyc.html`. Planning Department, Government of Rajasthan. Accessed: 2026-03-17.

[49] News18. e-KYC mandatory for Andhra Pradesh ration cards: Deadline set to complete process. *News18*, 2025.

[50] The Hindu. Deadline for ration card holders to complete e-KYC extended till June 30. *The Hindu*, June 2025.

[51] Times of India. e-KYC must for LPG subsidy beneficiaries every fiscal. *The Times of India*, 2025.

[52] Unique Identification Authority of India. The Aadhaar (authentication and offline verification) regulations, 2021. `https://uidai.gov.in/images/The_Aadhaar_Authentication_and_Offline_Verifications_Regulations_2021.pdf`, 2021. Notification No. K-11020/240/2021/Auth/UIDAI (No. 2 of 2021), dated 08.11.2021. Published in the Gazette of India, Extraordinary, Part III, Section 4. Updated as on 05.12.2024.

[53] Michael Safi. Personal data of a billion Indians sold online for £6, report claims. *The Guardian*, January 2018.

[54] MediaNama. Andhra Pradesh: Gang uses cloned Aadhaar-linked fingerprints to steal money from bank accounts. *MediaNama*, February 2023.

[55] MediaNama. Govt denies Aadhaar data leak, silent on questions of breach. *MediaNama*, July 2023.

[56] Lok Sabha. Unstarred question no. 2007: Leakages in Aadhaar database. `https://sansad.in/getFile/annex/259/AU2007.pdf?source=pqars`. 259th Session of Lok Sabha, Parliament of India. Accessed: 2026-03-17.

[57] DigiLocker. About DigiLocker: An initiative towards paperless governance. `https://www.digilocker.gov.in/web/about/about-digilocker`. Ministry of Electronics and Information Technology, Government of India. Accessed: 2026-03-17.

[58] Digital India Corporation. Digital India corporation: Driving India's digital transformation. `https://dic.gov.in`. Ministry of Electronics and Information Technology, Government of India. Accessed: 2026-03-17.

[59] Digital India Corporation. National e-governance division (NeGD). `https://dic.gov.in/negd/`. Ministry of Electronics and Information Technology, Government of India. Accessed: 2026-03-17.

[60] Open Source For You. Government leverages open source to build DigiLocker for Indian citizens. *Open Source For You*, October 2016.

[61] Charru Malhotra. DigiLocker: The digital vault of India. Technical report, National e-Governance Division (NeGD), 2025. Accessed: 2026-03-17.

[62] Ritul Gaur and David Eaves. The DigiLocker story: How India is digitising its documents. Case study no. 4, UCL Institute for Innovation and Public Purpose / Digital Impact Alliance, October 2025.

[63] DigiLocker. Organizational model. `https://www.digilocker.gov.in/web/organizational-model`. Ministry of Electronics and Information Technology, Government of India. Accessed: 2026-03-17.

[64] ownCloud. Government of India chooses ownCloud for DigiLocker project. *ownCloud News*, August 2016.

[65] Ministry of Electronics and Information Technology. Information technology (preservation and retention of information by intermediaries providing digital locker facilities) rules, 2016. `https://img1.digitallocker.gov.in/assets/img/digi_locker_rules_and_amendment.pdf`, July 2016. Notification No. G.S.R. 711(E), dated 21.07.2016. Published in the Gazette of India, Extraordinary, Part II, Section 3, Sub-section (i).

[66] DigiLocker. Terms of service. `https://www.digilocker.gov.in/web/about/tos`. Ministry of Electronics and Information Technology, Government of India. Accessed: 2026-03-17.

[67] Ministry of Electronics and Information Technology. Digital locker technology specification (DLTS) – version 2.3. Technical report, Ministry of Electronics and Information Technology, Government of India, March 2015. Accessed: 2026-03-17.

[68] API Setu. DigiLocker – technical resources for integration and secure document sharing. `https://apisetu.gov.in/digilocker`. National e-Governance Division (NeGD), Ministry of Electronics & IT (MeitY), Government of India. Accessed: 2026-03-17.

[69] National e-Governance Division. Partner organisation onboarding standard operating procedure (SOP) for DigiLocker. Technical report, National e-Governance Division (NeGD), Ministry of Electronics and Information Technology (MeitY), June 2024. Accessed: 2026-03-17.

[70] Digital India Corporation. Annual reports. `https://dic.gov.in/annual-reports/`. Ministry of Electronics and Information Technology, Government of India. Accessed: 2026-03-17.

[71] Digital Locker Authority. Steps to become a licensed digital locker service provider (DLSP). Technical report, Digital Locker Authority (DLA), Ministry of Electronics and Information Technology, Government of India. Accessed: 2026-03-17.

[72] DigiLocker. D.o. letter to dy. CAG regarding issuance of ePPO and GPF statements through DigiLocker. `https://www.digilocker.gov.in/assets/img/Circulars/DO%20Ltr%20to%20Dy.%20CAG%20reg.%20Issuance%20of%20ePPO%20and%20GPF%20Statements%20through%20DigiLocker.pdf`. Accessed: 2026-03-17.

[73] Times of India. Deadline for universities to upload academic data on DigiLocker set for December 31. *The Times of India*, 2024.

[74] Ministry of Education. Secretary letter regarding national academic depository (NAD). `https://img1.digitallocker.gov.in/nad/assets/circulars/SecretaryLetter_NAD_26June_2020.pdf`, June 2020. Government of India. Accessed: 2026-03-17.

[75] Yogesh Sapkale. Is the passport office enforcing DigiLocker via voluntarily mandatory Aadhaar? *Moneylife*, 2023.

[76] DigiLocker. DigiLocker policy. `https://www.digilocker.gov.in/web/about/digilocker-policy`. Ministry of Electronics and Information Technology, Government of India. Accessed: 2026-03-17.

[77] SecureBlink. DigiLocker vulnerability. *SecureBlink Cyber Security News*, 2020.

[78] Reserve Bank of India. RBI Central Board meets at Chennai: RBI to allow Account Aggregator NBFCs; to set up Financial Inclusion Advisory Committee. Press Release, July 2015. 552nd meeting of RBI Central Board chaired by Governor Dr. Raghuram G. Rajan. Press Release 2015-2016/27.

[79] Ministry of Finance, Government of India. Celebrating four years of launch of the Account Aggregator Ecosystem - India's Digital Public Infrastructure (DPI), September 2025. Press release marking 4th anniversary of AA framework launch (September 2, 2021).

[80] Reserve Bank of India. Master direction - Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016. Master Directions RBI/DNBR/2016-17/46, Master Direction DNBR.PD.009/03.10.119/2016-17, Reserve Bank of India, Department of Non-Banking Regulation, September 2016. PDF: https://rbidocs.rbi.org.in/rdocs/notification/PDFs/MD46859213614C3046C1BF9B7CF563FF1346.PDF.

[81] Reserve Bank of India. Draft Regulatory Framework for Account Aggregator Companies to Facilitate Consolidated Viewing of Financial Asset Holding: Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016. Draft directions, Reserve Bank of India, Department of Non-Banking Regulation, March 2016. Draft regulatory framework released for public consultation (deadline: March 18, 2016). Final Master Directions issued September 2, 2016. Press Release 2015-2016/2077. Full text available at https://rbidocs.rbi.org.in/rdocs/Content/PDFs/DNBF7CEC891AC90F45C38E5763B8E8AA1DAD.PDF.

[82] Malavika 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. Technical report, Future of Finance Initiative, Dvara Research, September 2020. Paper for the 2020 Central Bank of the Future Conference. Hosted at University of Michigan Center for Finance, Law & Policy. Available at: https://financelawpolicy.umich.edu/sites/cflp/files/2021-10/raghavan-singh-regulation-of-information-flows-as-central-bank-functions-implications-from-treatment-account-aggregators-india.pdf.

[83] Reserve Bank of India. Reserve bank of india (Non-Banking Financial Companies - Account Aggregator) Directions, 2025. Master Directions RBI/DoR/2025-26/368, DoR.FIN.REC.No.287/03-10-123/2025-26, Reserve Bank of India, Department of Regulation, November 2025. Consolidated and updated regulatory framework for NBFC-Account Aggregators, replacing the 2016 Master Directions. PDF: https://rbidocs.rbi.org.in/rdocs/notification/PDFs/368MDA3A72C813679452CB0A291E6B300DB59.PDF.

[84] Sahamati Foundation. Account aggregators in india, 2025. Lists 17 operational Account Aggregators licensed by the Reserve Bank of India (RBI) as NBFC-AAs.

[85] Department of Financial Services. Account aggregator framework, January 2026. Official government page on the Account Aggregator framework. As of December 31, 2025: 126 entities live as both FIP and FIU, 2.61 billion accounts enabled, 252.9 million users linked.

[86] Reserve Bank of India. Framework for recognising Self-Regulatory Organisations (SROs) for the Account Aggregator Ecosystem. Framework report, Reserve Bank of India, March 2025. PDF: https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/FEM12032025DBB0EC477F78498CB8165E44ACD656BB.PI

[87] NESL Asset Data Limited. Tariff. NADL is a wholly-owned subsidiary of National e-Governance Services Limited (NeSL), licensed by RBI as Account Aggregator.

[88] Vineet Ranjan, Lakhwinder Kaur Dhillon, and Gautam Negi. The transformative impact of the Account Aggregator Framework on Financial Inclusion in India: A Multi-sectoral Study of MSMEs, Microfinance, and Personal Lending. *Advances in Consumer Research*, 2(5):1623–1633, November 2025.

[89] Sahamati. Account aggregator ecosystem: Transforming india's financial services - adoption update. Ecosystem report, Sahamati, March 2025.

[90] Reserve Bank of India. *FAME (Financial Awareness Messages)*. Reserve Bank of India, Financial Inclusion & Development Department, Mumbai, India, fourth edition, February 2024.

[91] Reserve Bank Information Technology Pvt. Ltd. Rebit api specifications, 2024.

[92] Finarkein Analytics. Fiul: Financial information user layer, February 2023.

[93] S25 Digital. aa-client: Typescript library for account aggregator ecosystem, 2024.

[94] Setu (BrokenTusk Technologies Pvt. Ltd.). Setu account aggregator sandbox and api playground, 2024.

[95] Finvu (CookieJar Technologies). Finvu account aggregator api sandbox, 2024.

[96] Sahamati Foundation. Code of conduct for sahamati members, June 2025.

[97] Arundhati Ramanathan. Sachin Bansal's loan offer: Take money, let Navi peek into your bank account for years. *The Ken*, August 2024. Accessed: 2026-03-17.

[98] Reserve Bank of India. Master direction - Information Technology Framework for the NBFC Sector. Master Direction RBI/DNBS/2016-17/53, Master Direction DNBS.PPD.No.04/66.15.001/2016-17, Reserve Bank of India, Department of Non-Banking Supervision, June 2017. PDF: https://rbidocs.rbi.org.in/rdocs/notification/PDFs/MD53E0706201769D6B56245D7457395560CFE72517E0C.PDF.

[99] Government of India. The payment and settlement systems act, 2007. https://www.indiacode.nic.in/handle/123456789/2082, 2007. Act No. 51 of 2007. Enacted: 20.12.2007. Ministry of Finance, Department of Financial Services. Last Updated: 25.03.2019.

[100] Reserve Bank of India. Implementation of Bharat Bill Payment System (BBPS). Circular DPSS.CO.PD.No.940/02.27.020/2014-15, Reserve Bank of India, Department of Payment and Settlement Systems, November 2014. Original framework establishing BBPS; issued under Section 18 read with Section 10(2) of the PSS Act, 2007.

[101] Reserve Bank of India. Master direction — Reserve Bank of India (Bharat Bill Payment System) Directions, 2024. Master Direction RBI/DPSS/2023-24/111 CO.DPSS.POLC.No.S1114/02-27-020/2023-2024, Reserve Bank of India, February 2024. Effective 1 April 2024; supersedes the 2014 guidelines and all subsequent amendments; establishes the current comprehensive regulatory framework for BBPS.

[102] Reserve Bank of India. In-principle approval to NPCI for Bharat Bill Payment System. Press Release 2015-2016/1234, November 2015.

[103] Government of India. Companies act, 2013, 2013. Section 8 governs not-for-profit company incorporation; NPCI is incorporated under the predecessor Section 25 of the Companies Act, 1956.

[104] Reserve Bank of India. Second quarter review of monetary policy 2012-13. Monetary policy review, Reserve Bank of India, October 2012. Announced establishment of committee to finalise modalities for implementing an electronic GIRO payment system in India.

[105] G. Padmanabhan. Report of the committee to study the feasibility of implementation of Giro-based payment system in India. Committee report, Reserve Bank of India, 2013. Chaired by Shri G. Padmanabhan, Executive Director, RBI; estimated annual bill volumes exceeding 30,800 million transactions worth ₹6,223 billion in India's top 20 cities.

[106] Giro Advisory Group. Report of the Giro Advisory Group. Advisory group report, Reserve Bank of India, March 2014. Chaired by Prof. Umesh Bellur, IIT Bombay; recommended the tiered BBPS structure with a central standards body and multiple operating units; informed the final 2014 guidelines.

[107] Reserve Bank of India. Draft guidelines for implementation of Bharat Bill Payment System (BBPS). Draft guidelines, Reserve Bank of India, August 2014. Published for public comment; final guidelines issued 28 November 2014 "based on public comments received".

[108] National Payments Corporation of India. Technology infrastructure overview. Official website, 2024. Describes platform capacity of 8+ billion API calls daily (∼100,000 APIs/second) built on fully open-source solutions.

[109] NPCI Bharat BillPay Limited. NBBL developer program. Online portal, 2024. Provides certification pathway for Technical Service Providers; certified partners include Setu, PayU, Juspay, and BillDesk.

[110] National Payments Corporation of India. BBPS API specifications, version 13.0. Technical specification, National Payments Corporation of India, November 2019. Defines API interfaces for biller integration, payment modes, real-time transaction processing, and settlement services; access requires NPCI certification and MPLS network connectivity; exceeds 200KB in documentation size.

[111] NPCI Bharat BillPay Limited. Procedural guidelines for Bharat Bill Payment System, version 3.0. Procedural guidelines, NPCI Bharat BillPay Limited, March 2024. Defines roles of BBPCU, COUs, and BOUs; mandates TLS 1.2+ encryption and SHA-2 hashing; requires secure data archiving for ten years; references Annexure 8 (Compliance, Risk and Information Security).

[112] NPCI Bharat BillPay Limited. Bharat connect steering committee members. Official website, 2024. Lists current membership of the 15-member BBPS Steering Committee; NBBL serves as permanent member.

[113] Reserve Bank of India. RBI Digital Payment Index — March 2023. Press Release, September 2023. Index value 395.57 (March 2023) vs. 377.46 (September 2022).

[114] Government of India. Incentive scheme for digital payments in interim budget 2024. PwC India policy analysis, 2024. Allocates ₹2,600 crore for digital payment incentive schemes, including ₹3,000 crore for UPI P2M transactions and ₹500 crore for RuPay card incentives.

[115] NPCI Bharat BillPay Limited. Financial statements FY 2023–24, 2024. Reports total revenue of ₹8,566.58 crore (FY24), net profit of ₹2,726.17 crore, and profit margin of 31.82%; SGM contributions of ₹7,723.63 crore from member banks.

[116] L. Srikanth. Privacy risks in India's Bharat Bill Payment System. *Cashless Consumer*, 2020. Documents non-consensual retrieval of utility bill data by BBPOUs including PayTM, PayUMoney, Google Pay India, and HDFC Bank; identifies auto-fetching of data post-app-uninstallation; highlights use of bill-payment data for credit-score construction.

[117] National Payments Corporation of India. Falcon: Hyperledger Fabric deployment helper for Kubernetes, 2023. Open-source component released by NPCI; demonstrates contribution guidelines and labelled issue structure for community participation.

[118] Government of India, Ministry of Electronics and Information Technology. Information technology (reasonable security practices and procedures and sensitive personal data or information) rules, 2011, 2011. Prescribes security standards for handling sensitive personal data by body corporates in India.

[119] NPCI Bharat BillPay Limited. Privacy and security policy. Official website, 2024. Governs data collection and processing for Bharat Connect website users; covers financial and personal data categories.

[120] Reserve Bank of India. Master circular — Know Your Customer (KYC) norms / anti-money laundering (AML) standards / combating of financing of terrorism (CFT) / obligation of banks under PMLA, 2002. Master Circular RBI-2015-16-42, Reserve Bank of India, July 2015. Mandates active transaction monitoring for anomalous activity by regulated financial institutions.

[121] Indian Computer Emergency Response Team (CERT-IN). Directions under sub-section (6) of section 70b of the information technology act, 2000, relating to information security practices, procedure, prevention, response and reporting of cyber incidents for safe and trusted internet. Statutory Direction Direction No. 70B, Ministry of Electronics and Information Technology, April 2022. Mandates reporting of cybersecurity incidents to CERT-IN within 6 hours; covers 20 categories of reportable incidents; requires minimum 180-day log retention for all ICT systems.

[122] Government of India. The digital personal data protection act, 2023, 2023. Establishes a rights-based framework for processing digital personal data; implementing rules pending notification as of 2024.

[123] National Payments Corporation of India. Aadhaar enabled payment system (AePS) — product overview. Official website, 2023. Links Aadhaar numbers to bank accounts for biometric (fingerprint/iris) authentication; supports balance inquiries, cash withdrawals, deposits, and fund transfers.

[124] National Payments Corporation of India. Aadhaar payment bridge system (APBS) — product overview. Official website, 2023. Uses Aadhaar number as a financial address for routing government Direct Benefit Transfers; implemented in collaboration with UIDAI.

[125] National Payments Corporation of India. Cyber security at NPCI. Official website, 2024. Discloses certifications (PCI DSS v4.0, ISO 27001:2013, ISO 22301:2019, ISO 27701:2019, ISO 9001) and security infrastructure including Zero Trust Architecture and 24x7 SOC; references 2019 government audit findings.

[126] National Payments Corporation of India. UPI product booklet. Technical report, National Payments Corporation of India. Accessed via Internet Archive: `https://web.archive.org/web/20250415083211/https://www.npci.org.in/PDF/npci/upi/Product-Booklet.pdf`. Accessed: 2026-03-17.

[DRAFT — compiled at 2026-05-08 7:27; not for distribution]

[127] National Payments Corporation of India. Purpose and value. https://www.npci.org.in/purpose-value. Accessed: 2026-03-17.

[128] National Payments Corporation of India. UPI steering committee. https://www.npci.org.in/product/upi/steering-committee. Accessed: 2026-03-17.

[129] National Payments Corporation of India. NPCI's unified payments interface (UPI) set to go live August 25, 2016. https://www.npci.org.in/PDF/npci/press-releases/2016/NPCIsUnifiedPaymentsInterface(UPI)settogoliveAugust252018.pdf, 2016. Press Release. Accessed via Internet Archive: https://web.archive.org/web/20250907101107/https://www.npci.org.in/PDF/npci/press-releases/2016/NPCIsUnifiedPaymentsInterface(UPI)settogoliveAugust252018.pdf. Accessed: 2026-03-17.

[130] MediaNama. GPay is a third party app on UPI, not payment system: Delhi HC. *MediaNama*, August 2023.

[131] National Payments Corporation of India. Unified payments interface (UPI) procedural guidelines, 2019. Version 1.7, National Payments Corporation of India, 2019. Framed under the provisions of Payment and Settlement System Act, 2007. Dated 26.11.2019. Accessed: 2026-03-17.

[132] National Payments Corporation of India. Unified payments interface (UPI) procedural guidelines. Version 1.5, National Payments Corporation of India, July 2016. Framed under the provisions of Payment and Settlement System Act, 2007. Accessed: 2026-03-17.

[133] Reserve Bank of India. Storage of payment system data. https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11244&Mode=0, April 2018. Circular No. RBI/2017-18/153, DPSS.CO.OD No.2785/06.08.005/2017-2018.

[134] Sreenivas Ajankar. No more free UPI transactions? MDR charges likely to make a comeback. *Upstox*, March 2025.

[135] Ishika Gupta. Union cabinet approves rs 1,500 crore outlay for UPI transactions: What it means. *MediaNama*, March 2025.

[136] PhonePe. Business solutions in India. https://www.phonepe.com/business-solutions/. Accessed: 2026-03-17.

[137] Paytm Business. How brands can drive sampling through Paytm ads? *Paytm Business Blog*, June 2023.

[138] Razorpay. TPAP integration go-ahead: Requirements, process & benefits guide. *Razorpay Blog*, June 2025.

[139] Razorpay. How to register a PSP in UPI? – a detailed guide. *Razorpay Blog*, December 2024.

[140] National Payments Corporation of India. NPCI press release: BHIM app open source license model. https://www.npci.org.in/PDF/npci/press-releases/2022/NPCI-Press-Release-BHIM-App-Open-source-license-model.pdf, 2022. Press Release. Accessed via Internet Archive: https://web.archive.org/web/20250503060630/https://www.npci.org.in/PDF/npci/press-releases/2022/NPCI-Press-Release-BHIM-App-Open-source-license-model.pdf. Accessed: 2026-03-17.

[141] Ikigai Law. Payments, payments everywhere, not a dime to earn: Zero MDR & the disruption of the digital payments revenue model in India. *Ikigai Law*, May 2020.

[142] PwC India. Demonetisation effect: Digital payments gain new momentum. Technical report, PwC India, 2017. Fintech Insights. Accessed: 2026-03-17.

[143] Vikaspedia. News updates on digital payment promotion. https://en.vikaspedia.in/viewcontent/e-governance/digital-payment/policies-and-schemes/news-updates-on-digital-payment-promotion. Ministry of Electronics and Information Technology, Government of India. Accessed: 2026-03-17.

[144] National Payments Corporation of India. User onboarding on UPI. https://www.npci.org.in/product/upi/user-onboarding-on-upi. Accessed: 2026-03-17.

[145] National Payments Corporation of India. NPCI UPI OC 115: Rollout of numeric UPI ID mapper to enable UPI number. https://www.npci.org.in/uploads/NPCI_UPI_OC_115_Rollout_of_Numeric_UPI_ID_Mapper_to_enable_UPI_Number_c7ad12604f.pdf. Circular. Accessed: 2026-03-17.

[146] National Payments Corporation of India. UPI OC no. 115e FY 2024–25: Addendum to circular on the numeric UPI ID resolution. https://www.npci.org.in/uploads/UPI_OC_No_115_E_FY_2024_25_Addendum_to_circular_on_the_Numeric_UPI_ID_resolution_5bf6b7d3a5.pdf. Circular. Accessed: 2026-03-17.

[147] Indian Computer Emergency Response Team. Directions under sub-section (6) of section 70b of the information technology act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for safe & trusted internet. https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf, April 2022. No. 20(3)/2022-CERT-In. Ministry of Electronics and Information Technology, Government of India.

[148] The Print. Payments processor NPCI had over 40 security risks, user data vulnerable, says 2019 govt audit. *The Print*, July 2020.

[149] Nandan Nilekani, C. B. Bhave, R. Chandrasekhar, Dhirendra Swarup, S. S. Khan, P. R. V. Ramanan, and Nachiket Mor. Report of the Technology Advisory Group for Unique Projects (TAGUP). Technical report, Ministry of Finance, Government of India, New Delhi, India, January 2011. Accessed: 2026-03-31.

[150] Prashant Reddy T and Yogesh Byadwal. To whom is NPCI accountable? *The India Forum*, January 2026. Accessed: 2026-03-31.

[151] Press Information Bureau, Ministry of Finance, Government of India. DFS, M/o finance releases report titled "socio-economic impact analysis of incentive scheme for promotion of RuPay debit card and low-value BHIM-UPI transactions (P2M)" at chintan shivir 2026, February 2026. Release ID: 2228651. Accessed: 2026-03-31.

[152] Tanusha Tyagi. UPI at scale: Outages and the push for resilient systems. Observer Research Foundation Expert Speak, June 2025. Accessed: 2026-03-31.

[153] Prashant Reddy T. and Yogesh Byadwal. To whom is NPCI accountable? *The India Forum*, January 2026. Accessed: 2026-03-17.

[154] STQC Directorate. Rules and procedures for certification of digital locker service providers (DLSP)/dl repositories. Technical Standards DLCS-01-01, Issue-1, Ministry of Electronics & Information Technology, Government of India, Electronics Niketan, 6 CGO Complex, Lodi Road, New Delhi – 110003, January 2017.

[155] N. Ranganathan. The economy (and regulatory practice) that biometrics inspires: A study of the Aadhaar project. In *Regulating Biometrics: Global Approaches and Urgent Questions*, pages 52–67. AI Now Institute, 2023.

[156] A. Yadav. India's new data protection rules put state above privacy, imperil democracy and investigative journalism. Article 14, 2025.

[157] V. Bhandari and R. Sane. Privacy concerns in the Aadhaar Act, 2016. The Leap Blog, July 2016.

[158] A. Singh. NATGRID integrates with NPR database: What it means for privacy and law enforcement. MediaNama, December 2025.

[159] R. Bhatia. Critics of Aadhaar project say they have been harassed, put under surveillance. *Reuters*, February 2018.

[160] Outlook Web Bureau. UIDAI registers FIR against Tribune reporter over Aadhaar data breach report. *Outlook India*, January 2018.

[161] R. Garg. Don't penalise cybersecurity researchers! Internet Freedom Foundation, October 2021.

[162] T. Jalani. 7 million BHIM app records, including Aadhaar and UPI handles breached: VpnMentor. MediaNama, June 2020.

[163] M. Das. Cybercriminals 'cloning' Aadhaar biometric data to commit fraud: MHA nodal agency to states. The Print, March 2023.

[164] D. Aslesha and Z. Aafaq. Stolen fingerprints, empty bank accounts: How customers are paying for gaps in Aadhaar. Scroll.in, November 2023.

[165] B. Gonzalez. India deploys fingerprint liveness detection to combat Aadhaar payment fraud. Biometric Update, August 2023.

[166] R. Swaminathan. DigiLocker safety: Challenges and solutions. Moneylife, January 2025.

[DRAFT — compiled at 2026-05-08 7:27; not for distribution]

A Evaluation Framework

Ownership, operation, development considerations

1. How was the DPI launched (through an order, notification, legislation, etc?)
2. Who are the actors involved in conceptualizing the service?
3. Who are the actors involved in developing the service?
4. Who are the actors involved in operating the service?
5. What are their stated motives?
6. Were there public comments invited during the conceptualisation process?

Governance considerations

1. What metrics are being used to assess the success/failure of the DPI? (number of users, etc)
2. How are private players being encouraged to utilize the DPI/innovate?
3. Are there checks on limiting future applications of DPI (once a user has been enlisted for a specific purpose?)
4. What is the relationship between the private operator of the DPI and the government? (regulation, contractual arrangements?)

Economic considerations

1. Does the service operate on a profit model?
2. Are any of the actors involved in building or operating the service for-profit entities?
3. If there are for-profit entities involved, how do they make money off the service?
4. If there are non-profit / governmental entities involved, what programs fund their involvement in the service?

Openness considerations

1. Is the source code of the service available online?
2. Are parts of the source code available online?
3. Does the service provide open access to its API? If so, what functionality is enabled through the API?
4. Does software development happen in the open?
5. Does the service accept open-source contributions? Is there a clearly defined contribution policy?
6. Does the open-source project appoint maintainers responsible for managing open-source contributions?
7. Is there an open-source community around the service?
8. Can community members weigh in on design/development discussions?
9. Is there public reporting of operational status? (e.g., downtime dashboard)

[DRAFT — compiled at 2026-05-08 7:27; not for distribution]

Coercion

1. Is it mandatory to use the service?
2. If it is not mandatory, is there evidence of coercion/flouting of consent involved in the deployment?

Data collection practices

1. Is data collection governed by any privacy policies?
2. What data does the service collect from the user to sign up and use the service?
3. What data about the user does the service collect from other services? (e.g. KYC)
4. What user data is generated through usage of the service?
5. What metadata about the user is visible to the service?

Data storage practices

1. Where and by which entities is user data stored?
2. Are there any limits on data retention?
3. Does the service disclose information on data leaks? If so, what disclosure guidelines are followed? Does it report to CERT-IN and/or to users?

Data sharing practices

1. Does the service share data with any third-parties?
2. Is there a policy or reasoning provided for the data sharing?
3. Does the data sharing comply with privacy laws?

Data linking practices

1. Does the service explicitly link to any other service (e.g. Aadhaar linking)?
2. Does the service collect unique identifiers that could be used to link to records in other services (e.g. phone number)?
3. Is linking documented in a policy?
4. Does linking serve a legitimate stated purpose?

Security

1. Does the service make public statements about their security practices?
2. Is there a well-defined process to report security vulnerabilities? If so, how accessible is the process and are bug bounties offered?
3. Does the service disclose discovered security vulnerabilities? If so, does it report to CERT-IN and/or to users?

[DRAFT — compiled at 2026-05-08 7:27; not for distribution]