Internet Governance Project

India Stack:

Public-Private Roads to Data Sovereignty

TABLE OF CONTENTS

Introduction

With a total telephone subscriber base of 1.7 billion as of November 2022,[1] and 837 million Internet subscribers, India is the largest market in the world after China. A dizzying array of apps, services, and devices vie for Indians' attention. In 2021 India had 492.78 million smartphone users which increased to 647.53 million in 2022.[2] In 2021, India saw a stand-out 26.7 billion downloads of mobile apps and an average Internet data usage of 14.1 GB.[3] Smartphone users in India spend an average of about 4.7 hours or one-third of waking hours daily on various apps.[4]

The integration of digital technologies, content, and networks across all sectors has led to creation of large amounts of digital data. More and more analogue government and non-government data held in archives and repositories are being digitized and made accessible. Simultaneously, people interacting with a diverse set of information and communication technologies are generating growing quantities of digital data.

Even as the so-called "digital transformation" proceeds, nearly half a billion Indians have yet to come online. Between 2019-2021, India added more Internet subscribers in rural areas (95.76 million) than in their urban counterparts (92.81 million), and it is expected that by 2025 more rural Indians will be online than those living in urban areas.[5] Integrating this new community into the digital economy presents a profound challenge but also a tremendous opportunity and impetus towards enabling delivery of both government and private digital services to citizens.

Data, software, networks and digital devices are core components of the political economy in the 21st century.[6] However, their governance is being shaped in disparate international and domestic forums, laws and bilateral agreements. Various stakeholders including states with contending visions of who should have rights to various kinds of data, and how these rights can be exercised, are coming together to set norms, rules or agreements on governing data and cross border services that rely on the digital ecosystem.With the increasing importance of digital infrastructure and services, there is a growing body of work that has focused on understanding the digital political economy. As one element of a digital political economy,[7] critical data studies delve into specific histories, ideologies, and philosophies that shape data regimes and call attention to data's recursive relationship to power.[8]

With their first-mover advantage and scale, U.S. tech companies have users and buyers well beyond the U.S. borders. Initially, the U.S. government supported unrestricted flow of data across borders and pushed its partners to commit to promoting cross-border data transfers. However, the US-China trade war has resulted in the weaponization of global supply chains in the digital economy and a growing tendency toward China-targeted protectionism in digital services.[9] While President Trump was explicitly nationalistic, the Democratic Party in the U.S. also appears to have turned away from the liberal digital political economy,[10] and the Biden administration has several initiatives for data governance.[11]

Although China maintains tight control over information and communication services within its borders, digital technologies are also recognized as a strategic resource of production domestically, and driver of China's growing global ambitions. China has established a comprehensive cross-border data flow regulatory regime, the core of which is "local storage, outbound assessment." [12]

Europe does not have large technology companies of its own nor the market size of China or India. In an attempt to establish its role as a vanguard for digital policies and promote European values globally, it has adopted a regulation model that places an emphasis on the rights of users and prioritises data flows to countries whose legal systems meet their high standard of adequacy. The European Union's (EU) General Data Protection Regulation (GDPR) sets out these rights along with the legal mechanisms to enforce them. Simultaneously, the EU is also focused on companies meeting human rights and fair business conduct regulations as the Court rulings against the Safe Harbor and Privacy Shield arrangements [13] and the hefty fines being issued on tech companies across European courts demonstrate. With the introduction of the Digital Service Act and Digital Markets Act package [14] and the Data Governance Act [15] which goes into effect later this year, the EU is trying to create a single market for digital services and data.

Against this backdrop, *digital nationalism* or *digital sovereignty* have become prominent, and disputed, approaches of states seeking to control and regulate the digital economy.

Under this approach, the assertion of sovereignty by states is deemed essential for achieving an "ordered, value-driven, and regulated digital sphere." [16] Scholars have argued that claims of "digital sovereignty" emerged as a reaction to the globalisation of communications access by the Internet.[17]As the digital economy evolved and user bases expanded exponentially, states invoked the concept of sovereignty to counteract users in their country choosing platforms and services headquartered in the US. Similarly, *data sovereignty* frames the data of citizens as a national resource and encourages states to pursue policies that ensure sovereign control over this valuable resource.[18]

Digital technologies and data flows, however, challenge the territorial control and exclusivity invoked by political sovereignty.[19] Digital sovereignty is also inconsistent with the international division of labour and open trade in the production of software and information technologies that has emerged since the 1990s.[20] The large gap between nations' levels of technological development and the varying ideological notions of the role of the state, markets and individuals further complicates the application of sovereignty in cyberspace.

The primary aim of this paper is to understand how a sovereignty-based agenda is defining governance of data in India. We focus on data governance in India for two reasons. First, studying frameworks and approaches to governance of data is the perfect vehicle to highlight the transformation underway in the Indian digital economy. Second, India's approach to data governance blends both its external and internal strategies, and by focusing on data governance we can assess the effectiveness of the sovereignty-based approach in growing and leading a digital economy.

After reviewing relevant literature we decided to focus our efforts on studying the current administration's efforts to create a national digital public infrastructure under the India Stack umbrella.[21] India Stack is the moniker assigned to a set of APIs and associated platforms that operate across three critical sectors: identity, payments, and data. India Stack is claimed to be "national plumbing for the internet age" and "digital public goods" by its developers and supporters. The India Brand Equity Foundation (IBEF), a Trust established by the Department of Commerce refers to India Stack as *public digital infrastructure* and describes it as "the first national digital infrastructure in the world."[22]

Two of the technocrats behind this endeavour have described it as an attempt to use "technology to redefine government itself." [23] Others have described India Stack as "a unique platformization strategy by building public digital platforms across sectors" [24] and connected it to economic growth and empowerment.[25] Though India Stack was developed and implemented in India, its architects, developers and supporters have ambitions to export the "technology package" to other countries building "digital public infrastructure." [26]

India Stack APIs and solutions do not cover the full spectrum of the state's interaction with the notion of data sovereignty, rather they cover policy areas that are of relevance to the current environment and where India's sovereignty-based agenda to governing data is most visible. The key concerns which inform this work are India Stack's growing domestic and international influence and its framing as *digital public goods* or *digital public infrastructure*. In this paper we build on the issues and challenges highlighted by journalists, researchers, lawyers, social scientists, activists, and security professionals, many of which remain unaddressed.

After surveying relevant literature, the following are the big questions we want to answer through our study:

- When and why did the Indian government shift to pursuing a sovereignty based approach for the governance of technologies?
- How is India defining its sovereignty based approach to data governance?
- How does India Stack operationalize and take forward India's sovereignty based strategy for data governance?
- What policy problems are being created by a sovereignty based approach to data governance?

This paper will proceed through five main sections. Part 1 begins by sketching out the changing nature of technology development and governance in India, from the dominance of traditional firms to the state championing self-reliance to the current model rooted in sovereignty. Simplifying greatly, technology development and adoption in India has taken place through state-market cooperation. Part 2 introduces a conceptual framework to understand data sovereignty in India, the significant actors and the framings used in support of data sovereignty. In Parts 3 and 4, we track the creation of India Stack products, technical standards and governance systems and draw attention to the actors and interventions that have enabled these solutions to be created and deployed at scale. IGP argues that India Stack is rooted in India's sovereignty based strategy to extend its authority over the governance of digital data, resources, markets, and technologies. India Stack products, corresponding platforms and networks represent a deliberate attempt to embed hand-picked national champions in the creation and management of key processes or functionality deemed to be essential for operating in the digital economy.

Part 5 focuses on how India Stack solutions take forward India's sovereignty based agenda as well as broader commercial, political, and normative implications of India’s approach to building a digital architecture based on nation-state competition.

Part 1. Technology Development & Governance in India

In this section of the paper, we document India's push for the centralization of resources and control over electronics and information technology, in terms of both *rationale* and *process*. We believe that the logic of sovereignty has become a pivot point that guides India's agenda on digital issues. Consequently, this section focuses on situating India's assertion of digital sovereignty both contextually and historically. We outline the key actors and their motivations for pursuing and supporting sovereignty-based agenda in the digital economy with an aim of laying out systematic attributes of digital sovereignty more precisely attuned to the complex challenges faced by India. We situate 'digital sovereignty' as a phenomenon rooted in India's predisposition for state-centric approach to managing important domestic industries and the long-term tendency of pushing technological solutions to achieve India's economic and development goals.

The Roots of State and Market Cooperation (1950-60)

After independence, India was among the poorest countries in the world and faced a range of economic, social, and political challenges. Leaders and industrialists of the era were inspired by socialist ideas and supported state planning and interventions for development but also believed that rapid industrialisation offers the greatest scope of growth in production and improving the standard of living of citizens. State-led planning contradicts the market-based economy, yet the government in the 1950s adopted a strategy of economic development that combined aspects of both. India’s first Prime Minister, Pandit Jawaharlal Nehru is credited with creating and nurturing what is commonly referred to as the “Nehruvian Model of Development” which consists of four key dimensions: democracy, secularism, socialism, and non-alignment.

The Planning Commission was established in 1950 to formulate Five-Year Plans setting out specific goals and targets for different sectors of the economy. Left-behind British firms, the Imperial Bank (later renamed as State Bank of India) as well as important sectors like steel, mining, railways, airlines, heavy machinery, telecommunications, power were nationalized. In pursuit of self-reliance and creating a strong indigenous base in electronics and computers the government began investing in companies with the technological knowhow to design, develop and manufacture a whole range of electronic systems and equipment. However India soon realized the challenge of competing with commercial companies and shifted strategy to importing computers and electronics.

The second year plan along with the Industrial Policy Resolution (1956) laid the blueprint for industrialisation and development in India. Implementation of these policies and industrial development involved raising a massive amount of resources. A robust private sector that could catalyze investment was absent in India as a result of steady deindustrialization by Britain. Dedication to nonalignment made India wary of reliance on foreign aid or foreign capital. To overcome these challenges, the newly elected government established a strategy of state and market cooperation that continues to shape policy making today.[27]

The state acts as an investor and financier for the development of large state-owned industrial enterprises in critical industries. The state uses regulatory capacity to provide an edge to national champions, whether from the private or public sector. Demand for products and services developed by national champions is created by integrating their use in the public sector and government projects. The focus on the public sector aligned with the pursuit of "self-reliance" and the socialist goals of bringing the country’s productive resources under public ownership. It enabled the state to create new avenues of growth and take risks the private sector cannot afford. The private sector which had been calling for interventions and investments by the state to protect domestic industries supported and participated in setting up the public sector.

Protectionism and National Champions (1960-80))

In the 1960s and the 1970s India took first steps to liberalize the economy but continued with its protection of critical industries and creating national champions through the public sector. During this period problems resulting from this strategy of economic development started to become visible. For e.g. instead of creating an economic boost many public enterprises were unprofitable and strained government resources.

During the period of emergency in the country (1975-77) the government was willing to explore technological advancements, but was not enthusiastic about letting foreign firms operate without barriers. Efforts to expand computer design and manufacturing capabilities were confined to one public sector firm but several Indian companies entered the computer and computer-based services market. Computers were introduced in ministries and departments creating demand and a 'National Informatics Centre (NIC)' was established to coordinate and fulfill the government's computer needs.[28] By the end of the 1970s, it was clear that the license-raj had continued and India's policies were characterized as protectionist.

The government headed by Morarji Desai which came to power after Emergency was withdrawn, also prioritized the promotion of 'Swadeshi' or indigenous industries. Yet another public sector enterprise was set-up to fill in the vacuum created by IBM exiting India. Liberalized industrial policy enabled the emergence of several new players and the public sector was used to create demand for their products and services. By the mid 80s, the demand for homegrown hardware products reduced, and these firms shifted their focus to providing software and IT services.

Embracing Liberalisation (1980-90)

Moving away from the protectionist stance of the previous regime, the Rajeev Gandhi-led INC government which came to power in 1984 made some watershed decisions for software and computer industries. Import and licensing policies were liberalized, duties, taxes and tariffs reduced and foreign companies were permitted to establish fully-owned subsidiaries. Domestic and foreign companies operating in India came together to promote the sector's interests under the banner of the National Association of Software and Service Companies (NASSCOM). Simultaneously, backlash from local firms adversely affected by liberalization and changes in the political economy of the state resulted in the reversal of some earlier import liberalization.[30] By the late 1980s, policies regarding the computer industry had reached a stable middle ground, striking a balance between the protectionist approach of the mid-1970s and the liberalization measures of the mid-1980s.

India's embrace of liberalization resulted in the relaxation of import and licensing conditions to drive growth and investment in the IT sector. Domestic firms could raise capital through equity, were offered tax breaks and able to import hardware easily. The state invested in infrastructure and support to enable small and medium enterprises (SMEs) to develop and export hardware and software. These interventions enabled Indian firms to scale and enter global markets sparking an IT services export boom.[31] India's total software exports grew from USD 734 million in 1995-96 to USD 4 billion in 1999-2000. [32] Nevertheless, government spending continued to form the major part of investments and domestic demand was driven by the public sector.[33] Signaling the growing importance of telecom, and internet services for the economy, the Telecom Regulatory Authority of India (TRAI) was established in 1997 to regulate telecom services.[34]

Expanding State Control (1998-2004)

From 1998 to 2004, a centre-right coalition government called the National Democratic Alliance (NDA), led by the Bharatiya Janata Party (BJP), came to power. The BJP is a Hindu nationalist party affiliated with the Rashtriya Swayamsevak Sangh (RSS) a nongovernment organization propagating the values and culture of traditional Hinduism since 1925. The RSS and its economic wing, the Swadeshi Jagran Manch (SJM),[35] have been historically opposed to foreign trade and investment fearing that it could lead to economic or cultural domination.[36] The impact of liberalization on the economy had demonstrated that globalization could assist with the pursuit of economic security and self-reliance helping reduce resistance to foreign investment. Despite the protectionist roots of the BJP, the coalition headed by PM Atal Bihari Vajpayee was able to push through reforms that accelerated further liberalization of the economy.[37]

Support and financing from the government, improvements in infrastructure, and updated corporate laws paved the way for increased foreign direct investments and the entry of major e-retailers like Walmart and Amazon. India’s most overt trade barrier, customs duties, were reduced for a number of critical inputs in the IT sector such as micro assemblies, storage devices and CDs, telecom equipment and optical fibre. The IT industry’s contribution to the national economic output went from 1.2 per cent in the year 1997-98 to 3.5 per cent in 2003-04.

The period was also marked by growing domestic demand for software services. Although global IT companies operating in India offered a host of proprietary software and services, India's small and medium enterprises (SMEs) could not afford them. To fill the gap, Indian firms started focusing on production of reliable, affordable software to meet the needs of Indian businesses. The emergence of firms focused on domestic production marks an important shift in India's export-oriented software sector.

Following the 1999 India-Pakistan Kargil War, national security imperatives became an important element of regulation of the IT and communications sector.

Regulation of Communications Technology

The New Telecom Policy increased competition in the sector resulting in a gradual drop in voice calling rates and accelerating mobile adoption across sections of the society. The telecom policy separated the policy and licensing functions of Department of Telecommunication (DoT) from service provisioning and also clarified TRAI's role as an independent regulator with comprehensive powers. TRAI's authority to govern the telecom sector was strengthened through the TRAI (Amendment) Act, 2000 and its purview was expanded to include regulation of the carriage of television signals.

The Ministry of Communications and the Ministry of Information and Broadcasting (MIB) functioned as separate ministries. The Department of Electronics (DoE) was moved from under the PM and incorporated within the Ministry of Information Technology (MIT).[38] The NIC was moved from under the Planning Commission to the newly formed ministry.

Following the 1999 India-Pakistan Kargil War, national security imperatives became an important element of regulation of the IT and communications sector. The Information Technology Act 2000 (IT Act) was enacted to provide a legal framework for the use of electronic communications and digital transactions. The IT Act and changes to the licence agreements of Indian communications service providers expanded the government's power to seek interception, monitoring and decryption of all digital information electronically transmitted over India's telephone and Internet networks.

The terrorist attacks on parliament further intensified security concerns. In December 2001, the DoT was bought under the MIT which was renamed as Department of Information Technology (DIT). The government decided to issue a Multi-purpose National Identity Card (MNIC) to each citizen living in India and require them to register in a National Population Register (NPR). It amended the Citizenship Act in December 2003 to provide legislative backing to these initiatives.[39]

Tying Technology to Governance (2004-2014)

After no single party could get the majority, the INC-led United Progressive Alliance (UPA) came to power with support from other left-aligned parties between 2004-2008. The UPA regime led by PM Manmohan Singh was inwardly focused, prioritizing policies to assert state control over a rapidly growing economy. A number of policy measures were taken for supporting manufacturing of ICT hardware, telecom equipment, semiconductors, microelectronics and nanotechnology in India. The DIT was brought under the Ministry of Communications which was rebranded as the Ministry of Communications and Information Technology (MCIT).[40] In 2004 the National Broadband Policy was introduced to encourage creation and growth of network infrastructure. A framework to increase the penetration of .IN Internet domain names was introduced and the National Internet Exchange of India (NIXI) was established for its implementation. The National Cyber Security Policy was formulated and Indian Computer Emergency Response Team (CERT-In) made operational to protect critical information infrastructure and prevent cybercrime.

National Knowledge Commission

The roots of India Stack can be found in the National Knowledge Commission (NKC), a high-level advisory body to guide policy reforms for education, egovernance, science and technology.[41] Established in June 2005, the NKC was headed by Sam Pitroda, who as adviser to PM Rajiv Gandhi had helped build India's telecom and information technology infrastructure. It included representatives from the RBI, Indian Institute of Science, Tata Institute of Fundamental Research and Nandan Nilekani, the co-founder of Infosys, amongst others.

In December 2006, the NKC brought out a *Report to the Nation* covering recommendations on e-governance (e-gov) amongst other topics. The NKC then formed a special group, under the chairmanship of Nilekani, to study e-gov which recommended redesigning of government processes and procedures to “reduce the numbers and duration of successive steps required to obtain services” and “provide traceable records.”[42] To redesign government structures and processes, the group called for creating a central organisation with structures that can operate in mission mode with full autonomy and accountability. This centralised organisation would have a CEO and board members drawn from the IT industry and government.

After review by the Planning Commission and the MCIT, the NKC's and the special group's recommendations on e-gov were incorporated into the National e-Governance Plan.[43] The plan covered 27 Mission Mode Projects, including the creation of a national IT backbone, an Internet portal (India Portal) and Common Service Centers (CSCs) as access points for citizens. A separate department was carved out under MIT to take these projects forward.[44]

The UPA government allocated Rs 1200 crores[45] and the World Bank provided USD 500 million assistance for the Plan's implementation. ICICI Bank Limited an Indian multinational bank and Infrastructure Leasing & Financial Services Limited (IFSL) a government funded company helped create infrastructure. Software companies like IBM, HP, Oracle, Microsoft, and Tata Computer Systems (TCS) also contributed in various ways. Infosys CEO Nilekani (through the e-Government Foundation), and Wipro chairman Azim Premji (through the Premji Foundation) invested their personal wealth to develop and deploy e-governance projects by the state governments.[46]

Terror and Surveillance

In November 2008, a series of terror attacks planned and orchestrated by the Pakistan-based Lashkar-e-Tayyiba took place across Mumbai. The attacks, which soon became known simply as '26/11', lasted for four days, and exposed the strategic realities and deficiencies in India's counter-terrorism strategy. 26/11 was followed by immediate calls for the adoption of a hard approach to counterterrorism and modernisation of India's security and intelligence apparatuses.

The UPA, which had survived a 2008 vote of no confidence in the parliament brought on by the Left Front withdrawing its support, initiated a major institutional overhaul of the governmental architecture for handling terrorism in India. In December 2008 the National Investigation Agency (NIA) was established, expanding the state's investigative and surveillance powers.

A Central Monitoring System was set up to automate the process to intercept all communications on mobile phones, landlines, and the Internet in India by the government at will.[47] The Unique Identification Authority of India (UIDAI) was constituted to provide digital identity to residents. We cover the UIDAI in detail below.

In May 2009, the UPA alliance was elected to a second term. Coming to power in the wake of the Mumbai attacks, UPA-II was driven by the need to preserve India's strategic autonomy and territorial integrity and countering external and internal threats. It fast-tracked the Central Monitoring System, budgeting USD 150 million for the implementation of the system. In April 2010 the Cabinet Committee on Security approved INR 3,400 crore for the National Intelligence Grid (NATGRID), an intelligence sharing network that collects and collates data from the standalone databases of the various agencies and ministries of the Indian government. In 2013 Network for Space Objects Tracking and Analysis (NETRA) was introduced to intercept and analyze communications and Internet traffic using predefined filters.

The Global Financial Crisis

UPA-II's policies were also shaped by the need to ensure economic security. The global financial crisis had significant ramifications for the Indian economy. The immediate impact of the crisis was felt through large capital outflows and the consequent fall in the domestic stock markets, as foreign institutional investors sold assets and the Rupee depreciated against the USD.[48] As India's growth and exports fell sharply, policymakers had to step in to support the economy. The fiscal stimulus measures introduced by the government included both additional public spending as well as cuts in taxes.

The reduction in government spending slowed down the implementation of existing programmes and policies like the National e-Governance Plan which was suffering due to long, complex processes and lack of management expertise within the government. Delays in roll-out reduced the government's strategic control over resources, vendors, project outcomes and service levels. To help reduce procurement and implementation timelines, the government began exploring a Shared Platform for e-Governance balancing the benefits of centralization / standardisation with customization to suit business rules of ministries, departments and states."[49]

Central to the vision of the shared platform was designing applications using cloud-based architecture, integrating common shareable elements like UID authentication and payment gateways across domains, and using open APIs to allow innovations and new applications. The government hoped the shared platform would. The shared e-gov platform led to the creation of the National Computing Platform, a shared resource of reusable cloud-based software covering common processes to ensure interoperability between applications across government bodies and facilitate repurposing of solutions on demand. It included elements like National e-Governance Services Delivery Gateway (NSDG), State Service Delivery Gateway (SSDG), payment gateways, geographical information system (GIS) and APIs to enable delivery of government services over mobiles.

To address the lack of expertise within the government, the MCIT proposed creating a dedicated team staffed with domain and technical experts for the implementation of projects under the national e-gov plan. Each project team would be accountable to a ministry or department but would have operational flexibility, financial freedom and delegated powers for security or technology upgrades. Strategic projects would be staffed by internal resources with external hiring allowed only in special cases, after seeking approval from an empowered committee.

Alongside the development of the NCP and the MCIT's proposal, a Technology Advisory Group for Unique Projects (TAG-UP)[50] established by the Ministry of Finance and headed by Nilekani, recommended establishing *National Information Utilities (NIUs)*. As conceived by the TAG-UP, NIUs were a class of private companies with a public purpose that would work alongside the government to plan, design and implement complex IT-intensive public service projects. NIUs would participate in the planning or designing and work with the government in a vendor-customer mode to provide infrastructure and platforms required for the execution of public technology projects. The government provides strategic direction for NIUs, supports their development through policies or funding, and uses its authority to integrate their services into the digital economy.

The TAG-UP recommended structuring NIUs as a limited liability company with at least 51% private ownership and subject to corporate governance norms. The government retains strategic control over NIUs by virtue of being a shareholder and Board member and after the project is rolled-out and reaches a 'steady state', the government's role shifts to that of a customer. As a paying customer the government should "be free to take its business to another NIU", however TAG-UP acknowledges that given "the large upfront sunk-cost, economies of scale, and network externalities from a surrounding ecosystem, NIUs are essentially set up as natural monopolies." The references to the UIDAI and the National Payments Council of India (NPCI), scattered through the report and the common elements in the operational structure of NIUs and the NPCI and the UIDAI suggest these institutions provided the blueprint for the NIU framework.

Backing Away from Liberalisation

Regulating digital technologies was quite messy during UPA's second term. The involvement of a variety of institutions and organisations at various levels resulted in complex processes and tensions over control, deployment, and adoption of public and commercial digital technologies, services and industries.[51] The execution of digitization, broadband, e-governance and digital identity initiatives faced repeated delays. The UPA-II's ambitions of influencing global arrangements for digital governance were restrained by its slow learning curve.

The alliance was embroiled in fraud and corruption problems in the telecom, defence, coal and sports sectors, among others. Controversies emerged around UPA-II's policies on foreign market access and taxation of digital services. Politically, the Left parties and the Trinamool Congress[52] have been wary of the digital market economy and warned against the entry of foreign players. The BJP, then in opposition, was also vehemently opposed to the entry of large Chinese and American companies in the e-commerce sector.[53] Facing political pressure and ahead of the 2014 elections the UPA-II began slowly backtracking from trade liberalisation.

In the wake of the financial crisis, India's software exports slowed down and large IT firms with overseas operations like Accenture, Hewlett-Packard (HP) and IBM, were severely impacted by recessions in the west. However, major Indian IT firms that were primarily focused on exports as well as small and medium firms catering to domestic demand were able to turn the financial crisis into an opportunity for growth and expanding their reach. As global companies began to outsource work to reduce costs, they turned to Indian firms. IT firms like TCS, Infosys and Wipro were able to capitalise on the prior governments' investments in infrastructure to meet export demands. Production for exports grew faster than production for the domestic market even though domestic consumption of IT services was expanding.[55] As a result imports of communication and software services increased by 43.4% and 5% respectively, between 2013-14.[56]

As the profits of Indian IT firms focused on the export of IT software and services stabilised, they began to look for ways to expand but faced difficulties scaling up their services and products into other markets. Partner networks or mechanisms to enable Indian companies to access policy makers or navigate the maze of regulations in other countries were absent. The trade association formed in 1988 to promote the Indian IT industry, NASSCOM was perceived to be more focused on championing the multinational tech corporations than taking up the cause of domestic IT firms.[57] Lacking global visibility, Indian companies were being undervalued or ignored for acquisitions by foreign capital.

Indian software companies exploring ways to diversify from exports, shifted their focus to meeting domestic demand and inserting themselves into large government projects.

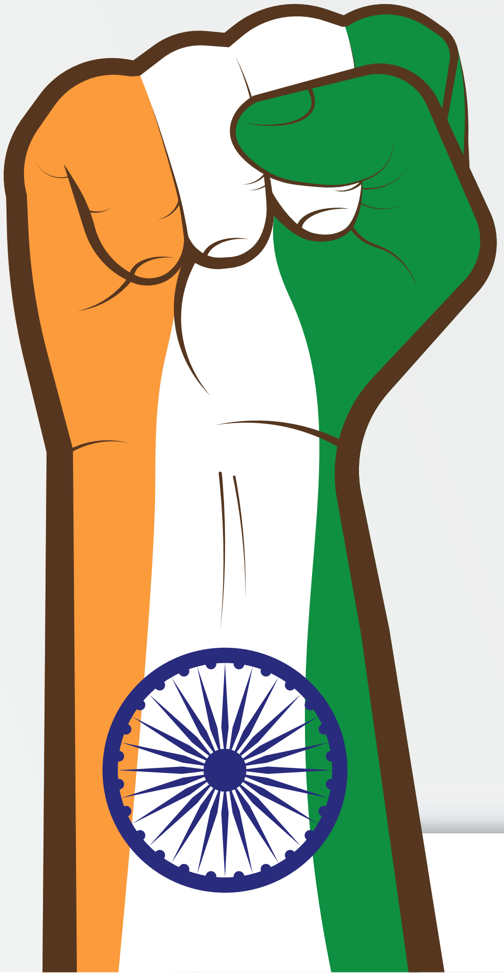
Against this backdrop, founders and executives of the best Indian software companies came together to establish the Indian Software Products Industry Round Table (iSPIRT) to promote the Indian software industry. iSPIRT was conceived as primarily a volunteer organisation with founders donating their time and money. It was decided that iSPIRT operate as a think tank and restrict itself to three areas: policy advocacy, creating reusable 'playbooks' of successful product strategies, and helping catalyse a market for software products.[58]

As some of iSpirt's early founders highlighted, "Bollywood is India's soft power. How could we make Indian [software] products the same?" iSPIRT attracted hundreds of entrepreneurs, developers, and investors, who as volunteers contributed their time and expertise out of a genuine desire to help the Indian software industry gain recognition.

Self-reliance and Sovereignty (2014-present)

In 2014, the BJP-led National Democratic Alliance (NDA) came to power. PM Narendra Modi's participation at the BRICS summit in Brazil, which led to the Fortaleza Declaration emphasising the sovereignty of States, indicated that the NDA government would follow the UPA regime in advocating for multilateral Internet governance.[60] However, the NDA government was able to shake off that perception by participating in the wholly multistakeholder NetMundial meeting,[61] and by unambiguously supporting the multistakeholder model during the IANA transition.[62]

In its first term, the NDA government was focused on positioning India as a global technology hub. India's foreign direct investment (FDI) regime was liberalised and investment restrictions reduced across sensitive sectors like defence, media distribution and the sub-sectors of retailing and e-commerce. These reforms resulted in a foreign investment boom. India attracted USD 33.8 billion in fresh foreign equity investments in 2014, which jumped to USD 40.7 billion in 2015 and USD 44.5 billion in 2016.[63]



Goal of Self-Reliance

Even as the government focused on attracting foreign investment, it latched on to the familiar idea that economic security required India to reduce its dependence on other countries. To achieve this vision of *Atma Nirbhar Bharat* or *Self-Reliant India*, the NDA government began to promote and nurture small and big business owners.[64] Atmanirbhar Bharat also lays special emphasis on technological self-reliance as a way to usher in a new industrial revolution in India.[65]

Self-reliance in the IT sector was promoted through two ambitious programs to support indigenous production of IT hardware and software for exports and domestic market. The Make in India initiative focuses on making India a hub for manufacturing by providing a conducive environment for companies to develop, manufacture and assemble products in India.[66] The Digital India program aims to create digital infrastructure to facilitate digital governance, service delivery and citizens' access to digital resources.[67] Existing policies and programs from the previous UPA regime, such as the National e-Governance Plan (2006), the National Optical Fiber Network (2011)[68] and Unique Identification Numbers (UID) (2009), were rebranded and consolidated under the umbrella of Digital India.[69] Additional programs like StartUp India,[70] Skill India, 100 Smart Cities,[71] 50 Metro Projects[72] and Swachh Bharat was introduced under Digital India.

Reinforcing State Control

In 2016, the MCIT which included three departments MIT (erstwhile DoT), DeitY and Posts was bifurcated into two ministries. The DeitY was made into a full-fledged ministry, the Ministry of Electronics and Information Technology (MeitY). Telecommunications, radio, telegraph and posts were brought under the Ministry of Communications.

In 2017, Media Lab Asia, a not for profit company established by the MCIT to bring the benefits of ICT to the common man was renamed as Digital India Corporation (DIC). The DIC role was to lead and guide the realizing the vision, objectives and goals of the Digital India program through promoting best practices, encouraging Public-Private Partnerships, nurturing innovation and technological advancements in various domains. Implementation of NeGP projects was handed over to DIC.

Expanding surveillance capabilities was a priority for the NDA government. India's surveillance projects like the Central Monitoring System, NATGRID, NETRA were continued. In 2015 the government issued a tender for the creation of a 'Social Media Communication Hub' to monitor social media networks. The tender was withdrawn after the media, activists and opposition leaders challenged the move in the courts.[73] In 2018, the Home Ministry issued a blanket order empowering 10 government agencies to monitor and decrypt information stored on computers on grounds of internal security.

As part of enabling widespread monitoring the NDA government prioritized and facilitated the development of digital identity and payments. The government went to the extent of opposing the Right to Privacy, and bypassing parliament in its support of these initiatives. In November 2016, the government withdrew all 500 and 1000 rupee notes from circulation, announcing the issuance of new 500 and 2,000 rupee banknotes in exchange for the now-defunct old ones. [74] These developments are covered in detail below.

Pursuing Sovereignty

The Modi government's push for the doctrine of sovereignty in the context of decision-making on Internet related activities was evident through but especially in the run-up to the 2019 general elections. The first official document which advocated for digital sovereignty to be a prime consideration for India's participation in the global economy was the 2018 National Digital Communications Policy.[75] The policy laid out strategies for ensuring digital sovereignty which included adopting a comprehensive data protection regime, upholding net neutrality principles, and building institutional capacity for developing security frameworks or standards and enforcing them.

The end of the NDA government's first term was marked by a wave of protectionist policies in multiple areas.

Investment caps blocking foreign firms from holding 100 percent of the equity of Indian companies were introduced across a range of sectors.[76] FDI was banned for certain sectors like inventory-based e-commerce.[77] Data localization mandates made data transfers prohibitively complicated and costly, particularly for foreign firms.[78]

After being re-elected with a convincing mandate, the BJP-led NDA alliance continues with pursuit of self-reliance, state control and sovereignty.[79] As part of the self-reliance campaign, India's budget for 2018–2019 was nakedly protectionist. Import duties were raised from around 10% to 15-50% on 40-odd items including mobile phones and accessories "to provide adequate protection to domestic industry" and "creation of more jobs."[80]

In 2020, the Department for Promotion of Industry and Internal Trade (DPIIT) made prior government approval mandatory for FDI from countries sharing a land border with India to prevent "predatory foreign investment" during the pandemic.

Manufacturing sector growth which was 7.8 percent annually between 2003-4 and 2013-14 increased to 9.1 percent between 2013-2014 and 2017-18, but then declined to almost a third at 3.4 percent in the last five years.[81] India's manufacturing sector contributed just 27.5 percent of India's GDP in 2019, the lowest in two decades indicating a gradual de-industrialisation of the Indian economy.

As part of the Make in India push, the NDA government has pushed policies incentivising global companies to move operations to India. The 2020 draft Data Centre Policy calls for locating data infrastructures within India "for protection of digital sovereignty." [82] India does not have native semiconductor manufacturing firms, but motivated by technological sovereignty and self-reliance wants to become a key player in the global semiconductor supply chain. The NDA has been focusing on partnerships and incentives to attract global chip makers to set up facilities in the country. In 2021 India approved a USD 10 billion incentive plan to attract investments for developing semiconductor and display manufacturing.[83]

India and the US have signed a memorandum of understanding on establishing a collaborative mechanism for the semiconductor supply chain resiliency and diversification.[84]

In 2022, India's exports of software services increased by 17.2 percent to USD 156.7 billion [85] and the country's share in global computer services exports was at a significant 10-11 percent. The government has also been championing a range of digital platforms and services developed through public-private partnership or by the private sector. A few countries in the world can match the scale of India's digital market, connectivity and access is unevenly distributed across geography, gender and income.

In 2021, compared to 69 percent in urban areas only 37 percent of the rural population and only one out of three women in rural India were active users of the internet. [86] The digital divide is perpetuated by low levels of digital literacy and lack of universal access to infrastructure. Government initiatives for laying of fibre and strengthening state networks continue to lag. Service-providers are limited in their ability to raise revenues due to the price-sensitive nature of the market, and consequently infrastructural investments remain low, impacting both access and internet quality. With decline in smartphone prices, there has been a sharp rise in the number of smart and feature phone users in India. However, given the low-income levels of large numbers of the population, affordability of internet-enabled devices continues to be an issue.

The government has introduced policies extending greater control over the communications technologies and media. In 2019 an Expression of Interest was floated for empanelling agencies which can track social media, monitor social media sentiments, segregate activities into 'problematic' and 'non-problematic,' make content go viral, and perform a range of other activities.[87] In 2021, the new IT Rules were introduced, altering the intermediary liability regime laid down under the 2011 Intermediary Guidelines and bringing digital media and streaming platforms into a stricter regulatory net.

The new IT Rules expands the powers of state and the obligations of digital platforms and service providers "for the protection of India's sovereignty and integrity". The legislation grants the government wide powers of censorship and interception powers particularly with regards to "significant social media intermediaries". Provisions to appoint an India-based office and officers for compliance and grievance redressal are aimed at enhancing the state's enforcement capabilities as failure to comply can land executives in jail.[88] Since its introduction, the IT Rules have been widely criticized for undermining and endangering individual freedoms, free expression, privacy and security. The legislation faces multiple legal challenges, with an Indian High Court having already stayed certain provisions due to the potential adverse impact on press freedoms. NDA-II has been using ad-hoc executive rulemaking to further amend these rules and create a content governance framework in India.

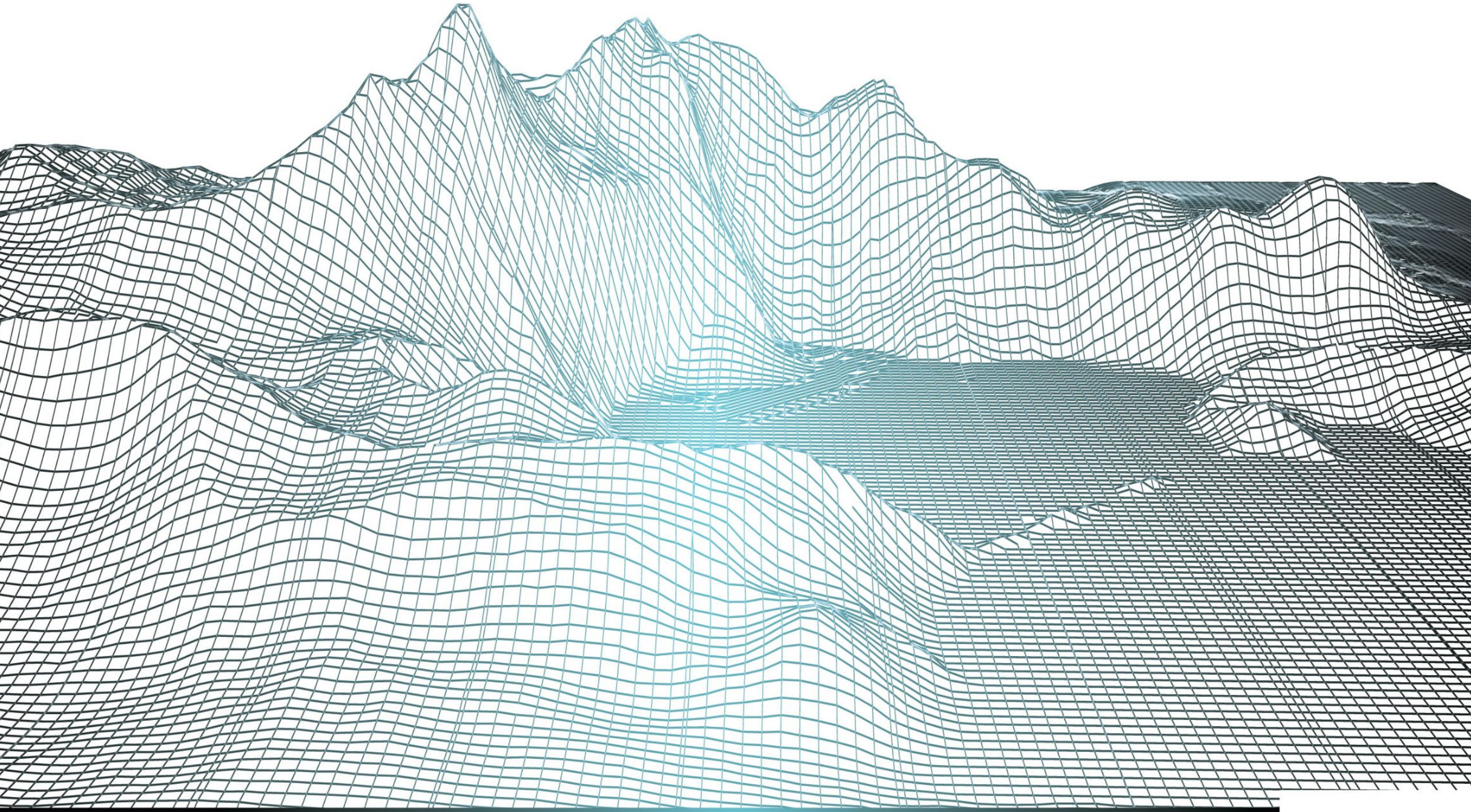
Following a tense border stand-off since June 2020 the deteriorating relationship between India and China has also impacted the NDA-II's policies. India reacted to Chinese military aggression by banning Chinese apps, claiming that they were "engaging in activities prejudicial to India's sovereignty, integrity, defence, security, and public order." India also cracked down on Chinese smartphone makers, allegedly for evading taxes. CERT-In, India's nodal agency for responding to computer security incidents has imposed strict data retention mandates requiring Virtual Private Network (VPN) and other service providers to retain user information for five years or longer.[89] The diktat has forced VPN providers to remove their servers from India and has been opposed by the IT and security industry, civil society, cybersecurity experts, and Indian SMEs.

India does not have a dedicated cyber security law and the government relies on sectoral ad-hoc legislation many of which are outdated and ineffective. Law enforcement agencies are unprepared to protect the digital economy from security vulnerabilities and emerging threats. India has the highest number of cyber crime like phishing attacks, financial frauds, mail-spams and ransomware attacks among G20 countries. In 2022, India accounted for 20 percent of all records exposed as a result of data breaches[90] with analysts estimating 92 percent of Indian companies having been breached.[91] The government has revealed in Parliament that cybersecurity incidents in India have increased from 0.2 million in 2018 to 1.39 million in 2022.

The Rise of Digital Nationalism

Over the years India's fragmented policy choices and shifting policy positions have created the perception that its decision-making has been ad-hoc and reactive rather than derived from a long-term vision. Characterising India's strategy from a mere bureaucratic and technocratic lens does not lend itself to the complex challenges India faces, nor does it allow for the development of a broader framework for the study of its Internet related policies. Key tasks for India are nation building and maintaining internal stability, which requires addressing poverty, strengthening the economy and protecting the country from external and internal threats.

As we have laid out above, the pursuit of these goals has led India to embrace both state-led and market-based strategies. Starting from post-independence industrial policy, India's predisposition for state control over key industries has remained a consistent theme. Simultaneously, struggling with resources and capacity has forced the state to embrace market-based reforms for economic growth and development.



The state played an outsized role in the development and adoption of IT and communications technology, acting as development agent, regulator, planner and promoter. The state's involvement was welcomed partly due to the lack of indigenous private entrepreneurs and partly due to economic distortions created by colonialism. Using a range of tools such as subsidies, tax incentives, infrastructure development,protective regulations, and R&D support, the state built up and promoted specific public sector companies, private firms and industries as national champions.

Setting up national champions is justified as a means to enhance national security by promoting self-sufficiency in key industries and ensuring economic growth by creating globally competitive companies. Although picking winners and losers has been successful in some cases, like the early computer and electronics industry and research centres, the approach can lead to market distortions. Despite the concerns, and driven by increasing economic nationalism and geopolitical tensions, establishing national champions continues to be an important strategy for the state to advance its interests.

India's assertion of sovereignty in the regulation of digital technology is rooted in its state-centric approach to managing important domestic industries. India has come to view digital technologies as being crucial for achieving these strategic and economic goals. Consequently,

economic prosperity, national security, sovereignty and digital technologies have become intertwined in the present government’s agenda.

Another important factor shaping India's turn towards sovereignty has been the rise of China. US-China trade wars revealed that even the world's largest digital economies are tying technological capabilities to national security, leading to neo-mercantilist forms of economic competition. The national security concerns arising from the border skirmishes with China have forced India to close its economy to Chinese investment, products and services, a decision which has been reinforced by the deteriorating US-China relationship.

India’s sovereignty-based approach to the digital economy is also motivated by its global aspirations and the larger geo-political agenda. As the global order changes and diversifies, alliances such as QUAD, BRICS, ASEAN and G20 become relevant for India from a geo-strategic perspective. This has led to efforts by India to balance its engagement with nations and actors that have conflicting agendas. As India aspires to be a leader or at least a rule-shaper with regard to digital technologies, it is pursuing sovereignty-based strategies with the objective of maximising its options to enhance its capabilities and maintaining strategic autonomy to secure its national interests.

Given these parameters and working with the assumption that sovereignty has become a pivot point that guides India's agenda on digital issues, in the next section we develop a framework to understand how India is using sovereignty to govern data.

Part 2.
When Nationalism and Data Converge

The importance of data in the digital economy has led India to view it as a strategic resource. India wants to achieve a $1 trillion digital economy and is betting on the size of its user population to generate data.[92]Both the UPA and the NDA governments have emphasised digitising all elements of its society, including information, goods, services, finance, manufacturing, health, personal identity and financial services. PM Modi has referred to data as "oil", "gold" and a "weapon." [93] The Indian Economic Survey of 2018–2019 dedicated a chapter to discussing the many benefits of data for policy making, welfare delivery, and product innovation.[94]

India's approach to governance of data is rooted in the idea that data originating within each country is a national asset and the state has the ultimate authority to regulate data within its borders. Outlining the shift in India's approach to data governance, ex-telecommunications secretary Aruna Sundararajan noted: "If data is the new oil, the future of our economic and national security will depend on our data regimes. It's essential that this data is available to Indians and Indian companies." [95]

Integral to the vision of Digital India is an attempt to extend and secure the state's power over the personal and non-personal data of citizens in order to pursue economic, social and geopolitical goals.[96] In July 2017, a committee of experts chaired by retired Justice B.N. Srikrishna was constituted to draft a personal data protection law for India. A slightly modified version of the Srikrishna draft bill was introduced as the Personal Data Protection Bill (PDP Bill) in the Parliament in December 2019 and referred to a joint parliamentary committee (JPC) for further consideration. After consulting with various stakeholders, the JPC published its report along with yet another draft bill - the Data Protection Bill, 2021 (DP Bill) in December 2021. The scope of the DP Bill was expanded to cover both personal and non-personal data. The bill was withdrawn, a new draft of the data protection law the Digital Personal Data Protection Bill, 2022 (DPDP Bill, 2022) was made available for public comments [97] and the government is expected to introduce the Bill in Parliament in the monsoon session of 2023.[98]

A committee of experts under the Chairmanship of G. Gopalkrishna was constituted to develop a framework for the protection and governance of non-personal data (NPD) in India released two drafts of its "Report on Non-Personal Data Governance Framework" first in July 2020 and then in November 2020.[99] Both versions established communities rights over data and recommended introducing data sharing obligations and creating data trustees to protect the rights of communities in relation to their non personal data. In February 2022 the government released the Draft India Data Accessibility and Use Policy to enable sharing of non-personal data and replaced the policy with the National Data Governance Framework Policy (NDGFP) in May 2022.[100]

Over the years a range of institutions and actors including political parties and business leaders, tech entrepreneurs and Indian companies that benefit from the strategy have started to extol the virtues of "data sovereignty". In 2019 Manch passed a resolution for ensuring sovereignty of data, data localisation, and digital nationalism.[101]Mukesh Ambani, India's richest man and Chairman of Reliance Industries, who views data as a "vital national resource", the "raw material" for the IT revolution and a form of "digital capital" has proposed a 'Keep in India' programme to preserve the nation's data within its borders.[102] Nilekani has noted: "Platforms that accumulate user data disrupt industries, wield disproportionate influence and create silos. This leads to data domination. The world is just waking up to this. India should too."[103]

India has clearly pushed data sovereignty through policies not only at home but, increasingly, advocated for the principle in international digital governance. Generally India supports open data flows—but as noted above it is increasingly taking steps to promote local technology firms and domestic control over data. At the close of June's G20 summit in Japan, India stood with a number of developing countries that refused to join the the Osaka Track an international declaration[104]by like-minded G20 countries promoting freer trade in e-commerce. The Osaka track seeks international rule-making on the digital economy, especially on free trade in digital services, data flows and e-commerce. India's boycott is representative of the ongoing struggle by some countries to assert a claim over their citizens' data.[105]

Despite the nationalistic turn, India seeks to increase access to services and choice for the Indian consumer base. India's participation in the Indo-Pacific Economic Framework for Prosperity (IPEF), the US's economic counterpart to its security efforts in the region, is an indication of its grudging acceptance that it can no longer sit on the fence on regulating digital trade and is open to building alliances and preferential trade networks. More recently, India is making digital technology governance a centrepiece of its G-20 presidency and promoting its ambitious "India stack" digitization project.

"Colonisation" and Data

India's colonial past is invoked to advocate against the dominance of foreign companies and justify the shift towards data sovereignty. Parallels are drawn between the colonial mechanism of resource exploitation[106]under British imperial rule and the economic practices of foreign technology companies.[107]Allowing foreign companies unrestrained access to data is framed as a new type of "data colonialism" which is not just economic but leads to "the enslavement of mind, body, and soul of the affected people."[108]A distinguishing feature of India's brand of digital neomercantilism is the use of nationalistic rhetoric, anti-corporate tropes by nationally based corporations with close ties to the government.[109]

The framing of data colonisation or imperialism resonates in India because of its traumatic historical experience with living under colonialism, and its success in overthrowing it. For advocates of this narrative, public policies should protect India's digital national champions and grant them exclusive access to Indian citizens' data. The parallel to "colonialism" in data is applied despite the fact that data exchanges among the world's peoples are not comparable to military occupation or violent subordination. The framing distracts attention from the problem of surveillance and control by India's own government.

Data "Empowerment"

The framing of "data empowerment" or giving the user more control as a tool of empowerment is also deployed in the pursuit of data sovereignty strategies. Various institutions and actors are pushing the data empowerment idea. The World Economic Forum (WEF) defines data empowerment as individuals having a say in how their data is used by organisations, and having the capacity to use their data for their own purposes.[110]

In India, this idea found its way into the Justice Srikrishna Committee 2018 report. It stated, "a free and fair digital economy that empowers the citizens can only grow on the foundation of individual autonomy, working towards maximising the common good." This framing of data empowerment is rooted in the idea of individual autonomy, a key tenant of privacy. Under this model, aside from providing consent, users are expected to engage in collective action to govern data. This expectation is not entirely compatible with the idea of privacy as individual autonomy; one is an individual right, the other a collective right.

Data empowerment shifts data management models from organisations to individuals. They are supposed to promote control by the users over the collection and sharing of their data, as individuals.[111] The data empowerment approach challenges state-centric data sovereignty. Given autonomy, individuals might choose foreign information service providers over national ones.They might prefer to store their data in clouds run by foreign companies. Advocates of state-centric data sovereignty often conflate the autarchy of the state with the autonomy of the individuals, when the two produce completely different sets of incentives. Sovereignists try to square this circle by promoting the state as a "custodian" of citizens' data rights.

Data empowerment also sometimes implies a strategy of assigning individuals property rights over their data so that they can benefit economically from it. Data empowerment can mean that users should have the power to withhold or approve the use of their data and engage in various forms of bargaining, including sale, to exploit its value. As far back as 2012, a government appointed committee on privacy headed by Justice Ajit Prakash Shah recognized that "data has economic value, and global data flow generates value for the individual as data creator, and for businesses that collect and process such data." [112]

The 2018-19 Economic Survey calls for a robust infrastructure for data management "can empower every stakeholder in society, from the Central Government to a local government body, from citizens to the private sector." The idea that data should "empower the individual, not the state, or the companies" has gained currency in business circles with prominent industry leaders calling for state interventions to "invert the data and put it in the hands of people." [113] Policymakers utilize the data empowerment discourse to project India as a digital leader in developing democratic models for the digital sector.

By promoting user control over data and by seeking ways to allow the value generated by data to be captured by the user, data empowerment in practice would work against state sovereignty. In India, however, notions of individual empowerment are used to rationalise the state exerting control over data and framing data nationalism as something states do for the sake of empowerment of their citizens.

India's Two-Pronged Strategy: Restrict, Accumulate

At home, India is extending state control over companies that generate and use the data of its citizens. It is promoting national champions and local ecosystems with the aim of making them challengers to the dominant players in the data market. Abroad, it advocates for the principle of data sovereignty in international digital governance and promotes the slogan "data by the people, for the people" at various forums.[114] At the same time India wants to be considered a destination for foreign direct investment and wants to enter the markets of other countries in the region, goals that obviously conflict with data nationalism. Given these different goals,

India's data sovereignty strategy has two elements: control that is exercised by placing restrictions on data; and accumulative strategies intended to enable the creation and sharing of data.

Restriction

Under the first prong of its strategy, India implements data sovereignty by laying down institutional arrangements and policies that restrict access to and sharing of data, or limiting its import and export. The link between data and territory is emphasised to limit access to data to entities based in India or handpicked foreign companies, and to drive forced localization measures to compel companies to relocate all or part of their global business operations within a country's borders. Restrictions on data are framed as measures that are necessary to prevent colonisation of data by foreign firms.

Nationalistic restrictions are often justified as responses to privacy violations, or as an attempt to apply national laws to data-generating companies located outside the country. The Srikrishna committee recommended localisation of certain categories of personal data. Numerous iterations of the personal data protection (PDP) bill severely limit data processing, place excessive restrictions on cross-border data flows, and include wide governmental powers to use personal data.[115] Data protection and privacy concerns are also used to restrict foreign access to non-personal data (NPD); that is, data generated by machine-machine communications, or measurements of the environment. The Gopalkrishna committee established that NPD derived from personal data, such as anonymised data aggregated for the delivery of services like ticketing, groceries, electricity or mobile phone use would "inherit the sensitivity of the underlying personal data." Such data has to be kept in India.

Under this prong, data is presented as most secure if it is located in the territory where it is being generated. India is forcing localization of a growing range of data types and services: in broadcasting, health, biometrics, banking, insurance, payments, mapping and location. The Consolidated FDI Policy, released in 2017 under the conditions for the broadcasting sector prohibits licensed companies from transferring databases and from processing subscriber data from the broadcasting sector outside India unless permitted by relevant law.[116] The 2017 insurance regulations require original policyholder records to be "held in data centres located and maintained in India only."

Other restrictions are justified by reference to data's link to national security. One National Security Advisor said that "data floating in cyberspace is a gold mine for extracting information that can ... add to the vulnerability of protected

information of the government and data concerning our critical infrastructure." [117]
PM Modi supports "servers being based in India and less dependence on foreign countries." [118]
Security concerns are also used to target the services of foreign firms. MeitY blocked numerous Chinese-owned apps, including TikTok, WeChat and QQ International on the grounds that the "compilation of these data, its mining and profiling by elements hostile to national security and defense of India ... impinges upon the sovereignty and integrity of India [and] requires emergency measures." [119] More recently, India has banned 14 messaging and file storage services on grounds of security threats arising from Pakistan.[120]

Security concerns are used to extend control over new categories of data and technologies. The Data Protection Authority established under the PDP Bill (now withdrawn) would have designated entities whose actions "are likely to have a significant impact on electoral democracy, state security, public order, or India's sovereignty" as "significant data fiduciaries" and subject them to greater compliance obligations, like mandatory data protection impact assessments, record keeping and audit requirements. In April 2022, CERT-In, the government- appointed agency tasked with performing cybersecurity-related functions, directed all entities that come under its authority to enable and maintain detailed logs of ICT systems for 180 days within the Indian jurisdiction.[121] By fostering surveillance of individuals' Internet activity, these regulations directly work against the claimed privacy concerns of the government.

Accumulation

Under the second prong of its strategy, India implements data sovereignty by introducing institutional arrangements and policies to enable public and private companies, especially national champions, to access and share data. The link between data and ownership is emphasized to drive efforts to develop a data market for personal or non-personal data. Data is framed as property and treated as an exchangeable, tradeable, and ownable resource that individuals, communities and the state must exploit to generate economic, social and public value. Property and ownership framing is also used to bring in familiar market-based concepts like commodity exchanges into data governance frameworks.[122]

Accumulation of data by the state and hand-picked national champions are often justified as efforts to enable individuals and communities to assert ownership over their data. This framing assumes individuals and communities generating data are by default the owners of their data and consequently have rights over their data including how their data should or should not be used. The principle of consent is used for operationalizing ownership over data, an approach that has gained currency as it appears to take forward tenets of privacy like individual self-determinacy and autonomy. Compelling individuals or communities to share data and participate in data markets is justified as efforts to enable "value" to be derived from data.

The government also relies on the doctrine of eminent domain, or the sovereign right to take over the property of an individual or community without their consent for the public good, to accumulate data. Under this approach, the state grants itself rights over the personal and non-personal data produced by its citizens or within its territory. By extension, the state has the power to compel and enterprises to "open up" data resources, and facilitate the development of data service industry for the benefit of its citizens or the public good.

Based on the recognition that “most data are generated by the people, of the people and should be used for the people,” the Economic Survey 2018-19 pitched the idea of treating repositories of government data as a “public good” for the benefit of citizens.[123] The survey does not distinguish between personal and non-personal data but notes that “enabling the sharing of information across datasets would improve the delivery of social welfare, empower people to make better decisions, and democratise an important public good”. It acknowledges that it is possible to exclude people from accessing data but recommends that “some kinds of data – particularly data gathered by governments on issues of social interest – should be democratised in the interest of social welfare.” “Democratized” seems to mean open access to NPD, much as the U.S. government handles census, weather, population data or other social statistics.

In July 2018, the Department of Industrial Policy and Promotion (DIPP) circulated a draft e-commerce policy requiring foreign companies to share data with Indian companies to gain market access. This proposal was retracted after strong opposition from key stakeholders. Another draft of the e-commerce policy released in 2019 declared the data of a country to be a national asset that the government holds in trust.[124] It proposed localization measures to keep data secure, enable Indian citizens and companies to extract "economic benefits from the monetization of data" and for “India’s data to be used for the country’s development."[125] The policy was retracted after strong opposition from key stakeholders.

In February 2022, MeitY released a draft of the India Data Accessibility and Use Policy which provided for the sale and licensing of datasets of public data available with various government departments and ministries to the private sector for commercial purposes. The policy was withdrawn after widespread criticism. In May 2022, MeitY released a new draft of the National Data Governance Policy Framework (NDGPF) with the aim of expanding the use of non-personal data and anonymized data from both government and private entities.[126]

The NDGPF provides “an institutional framework for data/datasets/metadata rules, standards, guidelines and protocols for sharing of non-personal data sets" to enable a start-up ecosystem based on Artificial Intelligence (AI) and data-based research.”[127] It calls for the creation of the India Data Council and an India Data Office within the Digital India Corporation (DIC) under the MeitY for the implementation of the policy. IMDO will consult with relevant stakeholders such as government ministries and state governments, to facilitate formulation and standardisation of guidelines and rules governing the management of datasets and metadata; and to accelerate inclusion of non-personal datasets and anonymized data sets of Indian citizens or those in India, housed within ministries and private companies into the India Datasets program. The policy is in the drafting stage and yet to be finalised.

The Gopalakrishnan committee has proposed a mandatory data sharing framework to utilise anonymised non-personal data created and held by public and private companies, to improve governance, research, and competition between businesses.[128] The committee has proposed that both government entities or private non-profit organisations take on the role of data trustees, acting as intermediaries to facilitate the exchange of data between businesses and between businesses and consumers.

To advance “communities’ rights over data that are relevant to them” data trustees can create high-value datasets (HVDs) by requesting access to data derived from a community [129] from businesses and after seeking approval of the Non-personal Data Authority (NDA). All firms active in the NPD market are obliged to share metadata of non-personal data which will be stored in a centralised directory, access to which will be managed by the NDA. Data trustees can identify opportunities and enforce sharing of data so communities and individuals and by extension the state can derive “social, public, economic value creation.” [130]

This approach of creating obligations for sharing of data conforms to common practice among democratic governments. Many forms of NPD should be treated as a commons, with free, nondiscriminatory access to members of the public, especially if it is produced with public money. If personal data is involved, there is a risk that anonymisation can be reversed. For this to happen, the data elements must be correlated with multiple other anonymized data sources to infer individual identity. This raises some privacy concerns. There are also other risks and ethical considerations associated with using data about individuals and communities from public datasets, for example, to assess their eligibility for other public and private services private data.[131] In the absence of robust institutional frameworks, use of public datasets containing personal or non-personal data falls in a gray area and has the potential to tip over into a biassed approach that hurts citizens especially, the most vulnerable.

Data sharing comes at a cost and creates an administrative burden which is more likely to be borne by large firms. Large firms are more likely to provide access to data but also have access to other sources of information on users and hence have higher marginal benefits from meta data. Since the goal of the policy is to to “disable the first mover advantage which leads to the establishment of walled gardens” the NPD set up suggests an asymmetric data sharing obligation.

In this section, I have developed a conceptual framework to understand India's sovereignty based approach to the data economy. I have shown how restriction and accumulation strategies are helping fortify data sovereignty in India. In the next section, I demonstrate how India is operationalizing data sovereignty strategies in the development of information infrastructures, domestic platforms and services.

Part 3. Foundations of India Stack

In this section, I highlight the convergence of a national digital identity system with money/payment systems. This convergence laid the foundations for India Stack. Though digital identity and payments systems are linked together under the umbrella of India Stack, each has an independent evolution shaped by a powerful combination of actors, motivated by different logic and objectives. India Stack is a product of converging organisational evolution as much as it is a product of a conscious policy or governmental strategy.

Linking Identity & Authentication

The foundations of India Stack were laid in the early 2000s around efforts to create a national digital identity. The Government of India first undertook an effort to provide a clear identity to residents in 1993, with the issue of photo identity cards by the Election Commission. Following the India-Pakistan Kargil War in 1999, a review committee appointed by PM Vajpayee identified illegal immigration as a concern and suggested issuing ID cards to improve border management. The Group of Ministers tasked to examine the committee's recommendations suggested compulsory registration of "citizens and non-citizens living in India" and introducing a national identity card based on documents like ration cards to solve the problem of illegal immigration.

Initially, the NDA government focused on smart cards to improve identity management and established a committee to formulate common standards for Multi-Application Smart Cards. Following the terrorist attack on the Parliament of India in December 2001, national security concerns intensified. This prompted the government to follow the Group of Ministers' recommendations and compel all citizens to register in a National Population Register (NPR). It also decided to issue a Multi-purpose National Identity Card (MNIC) to each citizen.[132] A pilot was launched across twelve states and one union territory.

Simultaneously, the government was deciding to integrate the Multi-Application Smart Card it has already started developing into India's welfare delivery architecture. In a country with poverty, unemployment, and a rural-urban divide, welfare schemes like subsidies and free ration distribution take on immense significance. The Public Distribution System (PDS) had been restructured in 1997, from a universal system, under which all Indians were eligible to receive a food subsidy, to a system that targeted those most in need. The shift to targeted delivery of subsidies would serve two main purposes: it would lower government expenditures, while reserving subsidies for those most in need. The delivery of subsidies through PDS was slow, difficult to access, and prone to manipulation or corruption.[134] There was rampant use of fake IDs or re-use of the same ID many times by individuals to divert benefits[135] To reform identification, the Department of Food & Public Distribution launched a Pilot Project on implementation of Food Credit Cards in PDS in Himachal, Madhya Pradesh and Kerala in November 2003.[136]

The pilots faced various hurdles: non-availability of data entry operators in regional languages; difficulty in capturing photographs and finger biometrics. Individuals in rural areas, especially agricultural labourers, landless labourers, married females or individuals not present at their place of residence, struggled to provide documents for determining citizenship status. Despite these issues, the Citizenship Act was amended in December 2003 to provide legislative backing to the National Population Register and MNIC initiatives.

The UPA government, which came to power in 2004 and had made digitising and streamlining government services a priority, decided to continue with the digital identity project, and began to explore integrating it into the delivery of other services or payment functions.[137] The 10th Plan Working Group on PDS and Food Security recommended replacing ration cards for accessing welfare services with the MINC, though the justification for doing so remains unclear.[138] In March 2006, the Department of Information Technology (DIT) approved a project titled "Unique Identification for Below Poverty Line Families" to be implemented by the NIC over a period of twelve months.[139]

A Processes Committee tasked to give shape to the project hired Indian IT major Wipro as a consultant for the design and program management phase of the project. Wipro prepared a strategic vision of the Unique Identification Number (UID) project, which has not been made available to the public.[140] An Empowered Group of Ministers was constituted to merge the UID project with the existing National Population Register and the MNIC project.[141] It took two years, but in January 2008 the Group approved the creation of a Unique Identification for Below Poverty Line Families by merging it with the National Population Register, MNIC, and establishing a UID authority to "own" the database.

Unique Identification Authority of India (UIDAI)

In January 2009, the Unique Identification Authority of India (UIDAI) was set up by executive notification as an attached office under the Planning Commision. Its key responsibilities were to generate and assign UID to residents, operate the database, manage the implementing agencies and "take necessary steps to ensure collation of National Population Register with UID".[142] In June 2009, Nilekani was appointed chairman of UIDAI and simultaneously given the rank of a Cabinet Minister.[143] As chairman, Nilekani hand-picked a set of "volunteers" from the private sector to develop UID facilitating "lateral induction of corporate leadership into the government."[144]

The government constituted a Prime Minister's Council to advise UIDAI and to ensure coordination between ministries, departments, stakeholders and partners.[145] On the back of very strong recommendations, civil servant Dr RS Sharma was appointed as the Director General and Mission Director of UIDAI.[146] Sharma had a background in technology and even wrote the first version of a client-software that was used to enrol people into the UID database.

Design of the Unique Identity (UID))

In April 2010, UIDAI published a Strategy Overview laying out the vision, design and implementation of the UID.[147] The document highlighted that the lack of a "nationally accepted, verified identity number" had created "identity silos" causing "extreme inconvenience" for citizens, and increasing the overall costs of identification. The UIDAI believed that linking an individual's personal identifying information to a UID number would create a standardised and reliable transaction identity for residents. The digital identity could be used by residents and agencies to verify identity for the transfer of money and resources.

As opposed to domain-specific identities, UID was conceptualised as a "root identity" or a "common identifier" designed to "give the government a clear view of India's population, enabling it to target and deliver services effectively, achieve greater returns on social investments, and monitor money and resource flows across the country." To prevent problems of identity fraud and duplicate or ghost citizen records from seeping into the UID database, the UIDAI decided to build a "clean database" with verified demographic and biometric information of residents. The UIDAI pushed the idea that seeding or linking existing databases with the UID would eliminate duplicates and allow databases to be cleaned at scale. [148] UID was also designed as an "authentication platform" that would perform a search on key demographic or biometric information of the resident to be matched with the record stored against the UID number in the central database.

Institutional Components of UID

UID has three primary components:
the enrollment ecosystem, the Central Identities Data Repository (CIDR), and the authentication ecosystem.

The enrollment ecosystem handles the onboarding of residents into the UID database, verification of their demographic and biometric details and issuance of a unique UID number. Residents can enroll through the National Population Register, or by submitting a proof of ID and address from a list of options drawn up by the UIDAI (passports, ration cards, voter IDs, etc.,) at Enrollment Centres (EC). Residents can enroll only once but may request their demographic and biometric details to be updated. The UIDAI put in place an introducer-based system for residents who did not have an extant identity or address document under which someone like the members of local administrative and elected bodies or the head-of-family can refer an individual for an entry in UID. [149] Outsourcing the problem of procuring the human resources needed for enrollment, the UIDAI partnered with various ministries, banks and public sector companies to act as Registrars that help enroll residents for UID numbers. Registrars conduct the enrolment camps, verify biometric and demographic data, upload the encrypted data to the CIDR to de-duplicate resident information and help seed the UID number into beneficiary databases. The UIDAI appoints Registrars, and each Registrar can employ Enrollment Agencies (EAs) to manage resources and operation of Enrollment Centres (EC). Registrars can appoint EAs internally for example, a bank may use its branches or appoint third-party vendors like the CSCs, a networked hierarchy of physical e-governance service centers spread across India.[150]

The CIDR is a centralised database that stores all Aadhaar numbers and corresponding demographic and biometric data. CIDR is also linked to deduplication as both enrollment and authentication processes must interact with CIDR to check for matches before generating a UID number for a resident or enabling them to use Aadhaar.[151]

The authentication facilities enable the use of Aadhaar to provide paperless identity verification for accessing services such as opening bank accounts, LPG connections, purchasing mobile SIMs, etc. An Authentication User Agency (AUA) can use an Aadhaar-based authentication facility to submit a resident's UID number, and a one-time password (or biometrics) as a second factor to authenticate identity. In addition to using Aadhaar-based authentication, a Know-Your-Customer User Agency (KUA) can use e-Know Your Customer (eKYC) authentication facility to retrieve a resident's signed and encrypted demographic record (name, age, address, etc.) from the CIDR.[152]

.

Technical Components of UID

The enrollment process had to be designed to allow offline enrollment to account for the lack of connectivity infrastructure in India. Registrars and EAs, which are the on-ground functional arm of the enrollment process, appoint operators to collect or update demographic or biometric data and verifiers to match the resident's documents with the details entered in the Aadhaar Enrollment Client. Both EAs and Registrars are required to use UIDAI approved equipment and follow guidelines and technical standards laid down by UIDAI.

The CIDR is distributed across multiple servers throughout India and is maintained, operated and owned by the UIDAI.

UIDAI offers several modes of authentication like biometric, demographic, two-factor or multifactor authentication and offline XML[153] and QR Code Scan.[154] The UIDAI standardises the authentication process through the use of APIs. Agencies using Aadhaar-based authentication and e-KYC facilities can connect to the CIDR through an Authentication Service Agency (ASA) and a Know-Your-Customer Service Agency (KSA) which own a secure connection through APIs which interact with the central database. The APIs are designed to work with applications written in any programming language, running on any computer or device, using any network including mobile networks. KYC details submitted by an Aadhaar holder which include the resident name, download reference number, address, photo, gender, DoB/YoB, hash of mobile number, hash of email are encrypted with a "Share Code" set by the user and downloaded as a machine readable XML file by the KUA. UID numbers collected by an AUA or KUA are encrypted and stored locally in a Data Vault.

The UIDAI chose "large scale distributed data stores for data management and analytics" that would allow "loose coupling of components" where changes could be made without affecting other parts of the system. It also created an "incentive aligned design" that enabled "use of multiple providers" and constant comparisons between them based on performance and cost. To eliminate vendor lock-in, the UIDAI opted for "open scale-out hardware architecture" built using open source technologies. Regunath Balasubramanian, one of the early members and primary architects of UID claims that use of open source software and open standards have enabled the project to achieve vendor neutrality and scale.[155]

While UID was built using mostly open source software, biometric de-duplication remains a proprietary component in Aadhaar. The companies that had been selected as vendors to enable biometric de-duplication would design, supply, install, commission, maintain and support the "multi-modal Automatic Biometric Identification System and multimodal Software Development Kit for client enrolment station, verification server, manual adjudication and monitoring function of the UID application."[156] The UIDAI created an API-based system to use proprietary software solutions from different vendors to perform biometric de-duplication and established " a management layer that can orchestrate across the multiple solution providers".

Three consortiums were chosen to provide the de-duplication hardware and software:[157]

- L1 Identity Solutions partnering with Hewlett Packard Enterprises and a recently set up Indian company 4-G identity solutions.[158]
- Mahindra Satyam partnering with Sagem Morpho the Indian subsidiary of Morpho Security Pvt Limited [159]
- US companies Accenture and Daon Inc partnering with Indian multinational MindTree. [160]

Implementation of Aadhaar

The UIDAI conducted a rushed proof of concept trial of the UID project between March and June 2010. It rebranded UID as Aadhaar (meaning 'foundation' in some Indian languages) and by September 2010 the first Aadhaar numbers were being issued to residents. The initial claim was that Aadhaar was a voluntary facility. The failure to define the scope and boundaries of Aadhaar's application and a network of public and private agencies incentivised to make money by registering citizens into the database, helped Aadhaar enrollment pick up across the country.

Right from its inception, legal and social science experts, development economists, and civil liberties advocates flagged issues with the Aadhaar project, including exclusion and the "legality of implementation of the UID project before the law is enacted by the Parliament." Ignoring these concerns the UPA-II introduced the National Identification Authority of India (NIDAI) Bill in the Parliament to create statutory backing for UIDAI. The Bill was referred to the Parliamentary Standing Committee on Finance stated that the UID had been conceptualized with "no clarity of purpose," was "riddled with serious lacunae" and urged the government to reconsider the project.[161] Instead of addressing these issues, the government abandoned the NIDAI Bill but continued to implement Aadhaar without legislative or statutory backing.

The expansion of Aadhaar was taken forward by creating the impression that Aadhaar would soon replace alternative methods of identity verification like driver's licenses and voter ids was created by both the public sector and a private sector to push consumers into enrolling into the scheme. These efforts by the state created demand for Aadhaar, and as a result a range of public and private sector companies, like banks and telecommunications firms began integrating Aadhaar authentication and eKYC services for identity verification. The other peg which was used to create acceptability for Aadhaar's use by public and private firms was that Aadhaar would eliminate identity fraud and weed out leakages or corruption.

By linking the unique identity with eliminating fraud and corruption, the government was also able to introduce it in the context of welfare delivery. The government carried out a relentless promotional campaign claiming Aadhaar would enable inclusion by providing an opportunity for individuals and communities outside of the formal system to gain access to services. To perpetuate this view certain features like the introducer system were incorporated in the design of Aadhaar. By creating the impression that Aadhaar would be essential for accessing subsidies and benefits, the state was able to push large numbers of poor, marginalized and underprivileged communities which live below the poverty line to enroll in the scheme.

The Move to Cashless

Indians primarily relied on paper-based modes of transaction like cash, cheques, and demand-drafts (DD) for payments and settlements. Settlement in the case of cash was instant and for cheques or DDs could take up to a week. Diners introduced credit cards to India in the 1960s, but its use was limited to people who lived or travelled to foreign countries. Indian adoption of credit cards was so slow it took the Diners Card fifteen years to reach 8,000 registered users. VISA and MasterCard were introduced to Indian consumers in the 1980s but their use was limited to high-income individuals. By 1993, however, almost all banks in India were issuing credit cards to their customers.

The growth of the credit card industry led to increased availability of ATMs across India. Taking advantage of the ATM infrastructure, banks started issuing debit cards to enable their customers to withdraw money anytime, anywhere. By the mid-1990s, use of credit and debit cards increased due to their acceptance at shops and competitive product offerings, which led the RBI to issue guidelines to banks for their issue in 1999.[162]

As cards gained popularity, banks began to view the big American card payment network operators as rivals and started to invest in technology to compete with them. For example, in 1997 the Industrial Credit and Investment Corporation of India (ICICI) bought the 'BankAway' software from Infosys to enable its customers to access banking services, pay bills, shop, trade and access a range of financial products and services over the Internet.[163]

The demand for instant payments, fueled by increased penetration of the Internet and smartphones, led to the emergence of digital wallets. The Reserve Bank of India classified digital wallets as Prepaid Payment Instruments (PPI).[164] Prepaid digital payment instruments have been around in India since 2002, but their use was restricted to gift cards, forex cards and the like. In 2004, Oxigen Wallet became the first digital wallet launched in India and was followed by several others like Wallet365.com, Mobikwik, Pockets by ICICI Bank and Paytm.[165]

Digitising Payments

The state acted as an investor to help RBI create payment systems to ensure reliable and secure electronic transfer of funds between banks.[166] The Special Electronic Funds Transfer (SEFT) enabled electronic transfer of funds between banks on the same day.[167] The Real-Time Gross Settlement (RTGS) [168] is a wholesale payment system to enable real-time electronic transfer of large-value payments between financial institutions. RTGS sets a minimum transfer limit of Rs 2 lakhs (approx. 2500 USD) and transactions are processed continuously and individually on a transaction-by-transaction basis.

The National Electronic Funds Transfer (NEFT) is a retail payments instrument that handles a large volume of low-value payments for purchase of goods and services by consumers and businesses.[169] These include person-to-person (P2P), person-to-business (P2B) like merchants, business-to-person (B2P) like salary transfers and business-to-business payments (B2B). NEFT operates on a deferred net settlement basis which settles transactions in batches and only at a particular point of time. NEFT does not set a minimum limit but may prescribe maximum limits per transaction.[170]

The RBI constituted a Board for Regulation and Supervision of Payment and Settlement Systems (BPSS) to lay down policies relating to the regulation and supervision of electronic, non-electronic, domestic and cross-border payment and settlement systems. BPSS is the highest policy making body for the payment and settlement systems. It sets standards for existing and future systems, approves criteria for authorisation of payment and settlement systems, and determines criteria for membership in these systems, including continuation, termination and rejection of membership. By the mid-2000s, most major banks in India had launched Internet banking services and the RBI was using the powers under the RBI Act, to regulate and frame guidelines for online banking services.[171]

In 2005 the National Payments Council was established to head reforms and propose [172] legislation for payment and settlement systems. The need for legislation was felt because the BPPS was operating without a legal basis and the formulation of core principles for Systemically Important Payment Systems[173] (SIPS). The Bank for International Settlements (BIS) classified payment systems that have "the potential to trigger or transmit systemic disruptions" as SIPS and laid down specific standards of regulation and oversight. Due to their impact in the form of systemic risks, the sole payment system in a country or systems that mainly handle time-critical, high-value payments are designated as SIPS and regulated by central banks. An RBI working group found the RTGS conformed to most principles for SIPS except a "well-founded legal basis" and recommended classifying it as such.[174] The RBI also recommended that the Working Group's classification of SIPS be reviewed from time to time.

Regulating Payment Systems

The Payment and Settlement Systems Act 2007 (PSS Act) came into force from 12 August 2008,[175] providing a legal basis for multilateral netting and settlements. Any system that enables payments between payer and a beneficiary and is involved in clearing, payment or settlement service qualifies as a 'payment system' under the PSS Act. The term 'settlement' has been defined, the terms 'payment' and 'clearing' have not been defined.

The PSS Act does not lay down a substantive legal framework for payment systems and is silent on issues like duties or obligations of service providers and system operators, as well as the classification of SIPS. [176] The Act designates the RBI as the apex authority, granting it the powers to issue directions or guidelines to deal with gaps in the primary statute.[177]

The central bank can implement measures such as capital requirements, licensing frameworks, fraud prevention mechanisms, and customer protection guidelines. The RBI can also impose penalties or take corrective actions against entities that fail to adhere to the prescribed rules and regulations. The RBI has the powers to authorize setting up or continuance of payment systems, but does not need authorisation to operate its own payment systems like RTGS, NEFT. The law does not specify whether banks are exempted from seeking authorisation for operating payment services.

Expanding Digital Payments Through Financial Inclusion

Despite the availability of multiple modes of electronic payments and growing acceptance by Indians, India continued to be a cash-based economy. This was due to several reasons.

The electronic payment and settlement infrastructure was slow and not widespread. By the late 2000s, RTGS and NEFT were the two primary modes for electronic transactions in India, but were available only during banking hours, and in some cases required manual intervention to process transactions. Friction in the banking system, and the lack of digital literacy limited the use of RTGS and NEFT to cities and urban areas, and mostly by citizens who already had access to the formal banking channels. For those without access or unable to afford formal banking, referred to as the "unbanked" or "underbanked," cash was the preferred mode of payment.

After the 2008 financial crash, prominent economists began linking the use of paper currency to tax evasion and illegal activity and promoting a "cashless economy."[178] The vision of a cashless economy held appeal for the RBI, which was exploring innovations and investments to expand the use of electronic payment systems.[179] Electronic modes of payments had evolved in a fragmented manner and were based on different proprietary interfaces, technical standards, communication protocols, supporting hardware, software infrastructure and operated under different business rules for accessing and protecting consumer data. This was beneficial for privacy as transaction data on users was maintained in silos. However, from the perspective of RBI and banks, the fragmentation of the market and lack of interoperability posed a barrier to widespread adoption of digital payments.

India's unbanked population constitutes a significant portion of the population and presents a large untapped market for the expansion of digital payments. In 2008 the Rangarajan Committee on Financial Inclusion set up by the Ministry of Finance noted that providing "access to finance is a form of empowerment of the vulnerable groups." [180] The committee called for constituting a multistakeholder National Mission on Financial Inclusion to take up the task of providing affordable financial services to all eligible sections of society or financial inclusion in a mission mode. [181] Two development and technology funds with an initial corpus of Rs. 500 crore each, contributed in equal proportion by the government, RBI, and the National Bank for Agriculture and Rural Development (NABARD) were established.[182]

National Payments Council of India (NPCI)

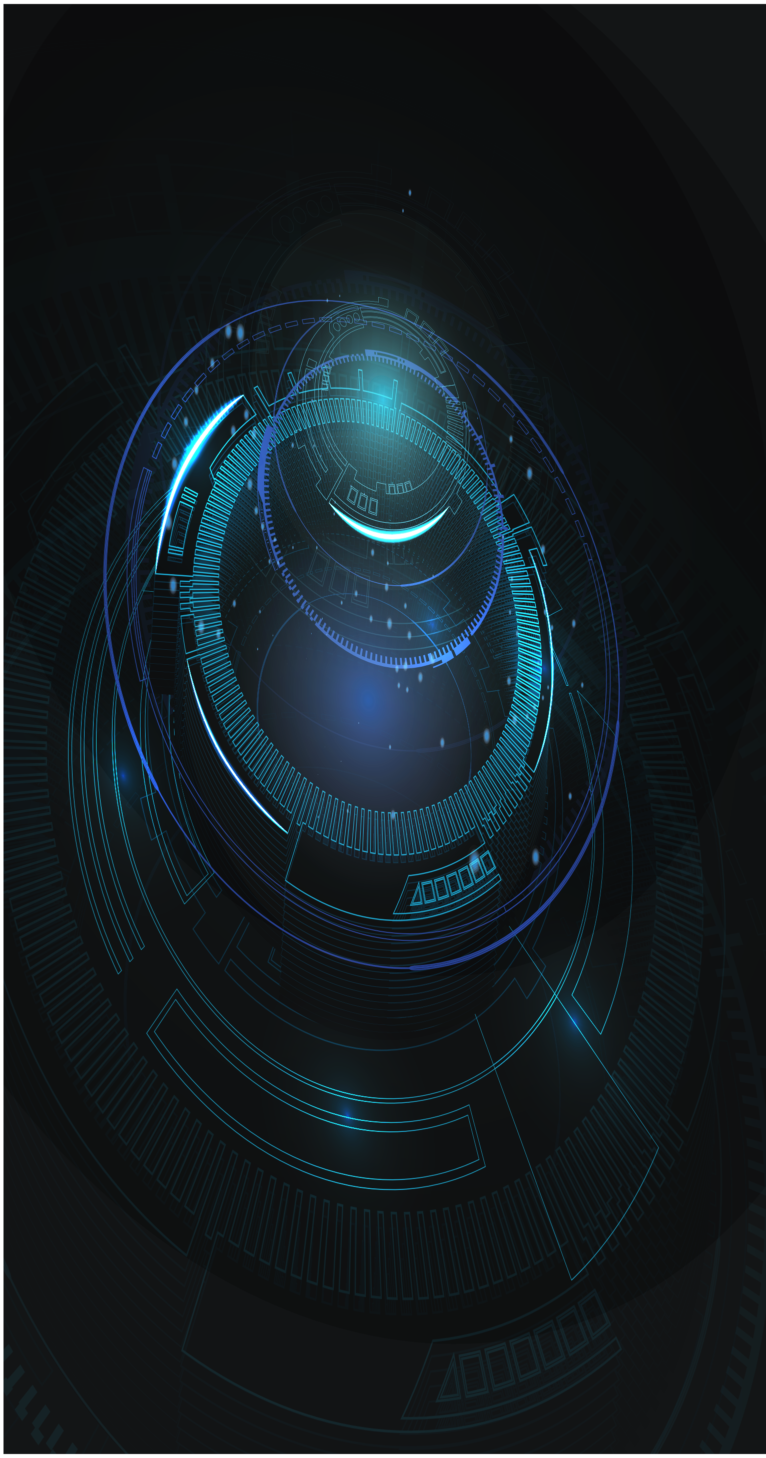
Traditionally, the field of payments in India has been bank driven. Banks were keen to retain their dominance over the business of transferring money digitally. Public sector banks also faced pressure to turn profitable since, as the majority stakeholder, the government was infusing public funds in their operations. In 2008, following the Rangarajan Committee recommendations, public and private banks operating in India came together to establish the National Payment Corporation of India (NPCI). The PSS Act empowers the RBI to authorize a "company or corporation" to " operate or regulate" existing or new clearing houses of banks, provided 51 percent equity of such a company or corporation is held by public sector banks. Taking into account this requirement, public sector banks have a majority stake in NPCI.

In September 2009, the RBI's Department of Payment and Settlement Systems (DPSS) gave in-principle approval to NPCI to operate various retail payment systems in the country. The RBI had estimated that government subsidies alone constituted more than Rs 2.93 trillion and if these payments were done electronically, it would translate to 4.13 billion electronic transactions in a year.[183] Additionally, there was scope for further electronification of other transactions like payments involving insurance, utility bills, taxes, school fees etc. to the government. The newly formed NPCI was directed to focus on facilitating the migration of payments and receipts of funds by government departments to electronic mode.

The NPCI began by expanding its membership by enrolling public and private banks in the country as members and created a membership structure. To standardize industry-wide adoption of payment systems the NPCI framed governance and regulations for member banks.[184] The NPCI was granted a Certificate of Authorization for operating the National Financial Switch (NFS) ATM Network, which it took over from the Institute for Development and Research in [185] Banking Technology (IDRBT) in December 2009.

In 2010, NPCI launched Immediate Payment Services (IMPS) an instant always-on, interbank funds transfer and retail payment system.[186] The system facilitates instant funds transfer of up to a limit of INR 5 lakh, on through mobile, Internet, ATM, or SMS. Besides banks, IMPS allows non-bank entities such as PPI issuers to participate and facilitate remittances from wallets to the beneficiary bank accounts over IMPS.

In 2012 the NPCI launched RuPay, a domestic card payments network to take on the Mastercard-VISA duopoly.[187]



Linking Digital Identity and Payments

The RBI constituted two working groups with members drawn from UIDAI, Indian Bankers Association (IBA), and NPCI to explore banking services to enable micropayments.[188] The UIDAI's involvement came from the UID being pitched as a transaction id that would transform "the large volume of micropayments, remittances and government transfers to UID-enabled bank accounts" into sources of revenue for banking institutions.[189] As explained by the UIDAI, building "an accessible, low-cost micropayments model" for financial inclusion would allow banks to access customers through several distribution channels for government including the mobile prepaid, post office, FMCG retailers networks and earn revenues from the large numbers of micro-transactions.

The working groups led to the creation of the Aadhaar-enabled Payment System (AePS). AePS allowed bank account holders to do Aadhaar-based authentication for accessing banking services at low cost interoperable micro-ATM networks across India.[190]

Another task force under the Chairmanship of Nilekani was constituted to examine and suggest "an implementable solution for direct transfer of subsidies

on Kerosene, LPG and Fertilizer to intended beneficiaries with the use of Aadhaar numbers, Aadhaar-enabled transactions and Aadhaar authentication infrastructure of the UIDAI." [191]

Within six months, the mandate of the taskforce was expanded to recommend and implement an Aadhaar-enabled unified payment infrastructure. The taskforce suggested that state and central governments: [192]

> Enable use of Aadhaar for Know-Your-Customer (KYC) requirements as a valid proof of identity and address. This would speed up the process of verification and provide a "portable" id that could enable "real-time authentication" anywhere, anytime. It would also do away with the paper-heavy documentation process that added to costs of services.
>
> Mandate the use of biometric authentication for certain schemes. This would push beneficiaries / customers to link bank accounts to Aadhaar. It would also boost Aadhaar seeding across government databases.
>
> Recognize Aadhaar as a financial address for receiving and sending funds. This would enable transfer of cash directly into Aadhaar-linked bank accounts of beneficiaries. Beneficiaries would be able to authenticate themselves at the last mile using Aadhaar-biometrics and banking correspondents.[193]

In May 2012, a Working Group of the Committee on Payment and Settlement Systems (CPSS), an international standard setting body for payment, clearing, settlement and related arrangements published its findings on Innovations in Retail Payments.[194] The committee found that innovations in payments were driven by opening up the market to competition from non-banks, and governments acting as a promoter of digital payments.[195] The report emphasized that integrating the unbanked or underbanked people into the financial sector or financial inclusion, whether mandated by the government or pursued as an opportunity to access untapped markets, was a key driver of innovation in payments.[196]

Since the prevalent model for financial inclusion in India was bank-led, the RBI, UIDAI, and NPCI latched onto the idea of developing retail payment instruments and infrastructure through the pursuit of financial inclusion. The RBI understood that the benefits of using financial inclusion for digital payments were not limited to welfare. The use of a central switch to move cash electronically at the last mile would dramatically cut down cash handling and other transaction costs for banking institutions.[197] Creating the demand for UIDAI and NPCI products and services, the RBI also permitted non-banks to offer prepaid payment solutions, such as cards, mobile payments, e-wallets and mobile wallets, with certain conditions.[198]

In late 2012 the UPA-II government announced the direct benefit transfers (DBT) scheme under which the government subsidies were to be replaced with cash transfers. The government argued that cash transfers would enable beneficiaries to avoid middle-men and would create a transparent and efficient way of ensuring that entitlements reach the correct beneficiaries. The advantages of cash transfers in the Indian context and the need for a unique ID were emphasised by the National Committee on Direct Cash Transfers.[199]

Legal Challenges to Aadhaar

The unrestrained expansion of Aadhaar's use in every sector, the grave consequences of authentication failures and the state's refusal to address challenges or slow down roll-out created pushback from activists and civil society, who called it the first step toward building a police state.[200] In November 2012, the constitutional validity of Aadhaar was challenged in a petition to the Supreme Court (SC) filed by (Retd) Justice K.S. Puttaswamy. A number of other challenges to Aadhaar were grouped with his petition.[201] Broadly the petitions argued that the project violated the right to privacy by creating the potential for mass surveillance. Authentication constituted an “unconscionable bargain” requiring citizens to part with their biometrics to access essential services and fundamental rights. The use of biometrics was unreliable and arbitrary, and therefore unconstitutional and the project’s implementation was a threat to personal and national security. The lack of involvement from state governments[202] contradicted the principles of federalism.

The Supreme Court expressed concerns about Aadhaar’s integration in the direct benefit transfer (DBT) scheme, its mandatory linkage to essential and nonessential services and Aadhaar cards being issued to illegal immigrants. Since state governments were continuing to mandate Aadhaar for accessing services from 2013-2017 the SC passed several orders directing the Union government to ensure that Aadhaar was not made mandatory for citizens accessing entitlements or benefits were not denied for lack of an Aadhaar number. Relatedly, the West Bengal government opposed linking LPG subsidy and passed a resolution asking for the Central government to delink Aadhaar from the direct benefit transfers scheme.[203]

Despite the ongoing challenge against Aadhaar, the Supreme Court orders [204] restricting the use of Aadhaar beyond Public Distribution, and the state governments interventions the Union government continued to demand Aadhaar but avoided the use of the term 'compulsory' or 'mandatory', urging consumers to "choose" Aadhaar for various services and purposes. Between January and March 2017, Aadhaar was linked with 22 government schemes.[205] A series of notifications made Aadhaar mandatory for services like opening a bank account - whether in private or public banks, buying a phone or a mobile connection, getting a passport, filing taxes or something as unconnected as school admissions.

Coming Together of RBI, UIDAI and NPCI

Ignoring the challenge against Aadhaar mounted in the SC, the RBI decided to capitalise on the government's decision to effect subsidy payments electronically rather than through cash transfers to proactively encourage the adoption of digital payments by people still not covered by banking products and services.[206] Building on the findings of the CPSS working group, the Rangarajan and Nilekani committees, the RBI published its vision for digital payments. It adopted a broad framework of "less cash/less paper society" under which it would pursue the complementary goal of financial inclusion. The vision statement advocated for state-market collaboration as "achieving the goal of inclusiveness and accessibility would require both banks and non-banks to play a complementary role" and would involve "devising an appropriate policy framework in which authorised private sector entities would play a significant role." [207]

To enhance the security of payment transactions and to address identity and address proof requirements, the RBI sanctioned the Aadhaar authentication (finger print, iris) and e-KYC services by UIDAI.[208] This was an important achievement for Nilekani who, as Chairman of UIDAI and the RBI taskforce, had been pushing for the integration of Aadhaar into the banking and financial sector to solve the unbanked population's lack of access and inability to provide verifiable identity documents. The UID strategy document had made the case for introduction of Aadhaar authentication and e-KYC in the banking sector to significantly reduce the documentation and costs of customer acquisition by banks. The RBI taskforce which he had chaired had recommended *Aadhaar being used as a financial address which would allow* residents to gain access to a UID-enabled bank account and funds to be transferred using the UID number.

The broader policies of the UPA-II government, various documents published by the RBI and UIDAI make it clear that policymakers and regulators had bought into Nilekani's idea from a few years earlier: "If we can get everyone to have a *UID number, bank account and mobile phone*, then we are giving them tools of opportunity. With that, they can *access services, benefits and their rights."* [209] The interventions from RBI, NPCI and UIDAI during this period indicate a deep collaboration between these institutions to embed Aadhaar in the digital economy.

Integrating Aadhaar, Banks and Mobiles

Following the announcement of the direct benefit transfers scheme, there was a massive push by the UPA-II government to make Aadhaar de facto compulsory under various government programmes involving transfer of cash including scholarships, pensions and wages.[210] UPA-II government also began pushing for integrating Aadhaar for welfare schemes that did not involve the transfer of cash like the Public Distribution System (PDS).[211] A pilot was launched in Andhra Pradesh to enable beneficiaries to access PDS rations by linking ration cards to Aadhaar and enabling Aadhaar authentication at "e-Point of Sale" (ePOS) machines.[212]

The RBI and other financial regulators certified Aadhaar as a valid KYC document for banking and financial services.[213] To integrate Aadhaar-linked e-authentication and eKYC services into the welfare delivery architecture, the NPCI developed several products. [214] The National Unified USSD Platform (NUUP) allowed people to access banking services by dialling *99# on their mobile phones and entering their bank Aadhaar number.[215] It launched the National Automated Clearing House (NACH), a web based solution to enable high volume, repetitive, periodic interbank transactions, and the Aadhaar Payment Bridge (APB) to link government departments and their banks to beneficiaries. NACH and APB enable government, financial institutions, and corporations to make payments and collect payments using Aadhaar.

Developing a national digital identity aligned with the NDA government's goals of self-reliance and expanding the use of digital technologies, products and services under programmes like Digital and Make in India. On 28 August 2014 PM Modi launched an ambitious national financial inclusion scheme - the Pradhan Mantri Jan-Dhan Yojana (PMJDY) - under which any citizen of India could use a mobile number and Aadhaar to open a Jan Dhan bank account and access financial services.[216] This was followed by the government aggressively promoting the adoption of the JAM trinity - Jan Dhan bank account, Aadhaar and mobiles for financial deliveries as a way to reduce cash usage, lower processing costs, and provide convenience. [217] The initial formulation of JAM trinity was linked to mobile banking and post office payments, the latter did not make much headway. The PMJDY proved that much like its predecessor, the NDA government and PM Modi had bought into the idea that Nandan had been pushing for years - the widespread linking of Aadhaar, mobile phones and bank accounts was necessary for inclusion and innovation in India.[218]

The PMJDY scheme provided a massive boost to UIDAI and NPCI's Aadhaar-enabled mobile banking strategy. In the first year 180 million bank accounts were opened under the PMJDY.[219] By 31 December 2014, over 730 million Aadhaar numbers had been issued and 100 million Aadhaar card holders had linked their bank accounts with Aadhaar.[220]To facilitate mobile banking, NPCI extended the NUUP *99# service for all telecom service providers in India. Other UIDAI and NPCI products were also integrated by banks under the PMJDY. Along with a PMJDY bank account, beneficiaries receive a RuPay Debit card, preloaded with insurance coverage of Rs 1 lakh. [221] Account holders can access financial services [222] using AePS.[223]

With Aadhaar's integration into the PMJDY and as enrollment crossed the 1 billion mark, the NDA government moved the UIDAI from under the Planning Commision and brought it under the former Ministry of Communications and Information Technology (MCIT). The Allocation of Business Rules were revised to attach the UIDAI to the Department of Electronics and Information Technology (DeitY) under the MCIT. [224]

Legal Roadblocks & Statutory Backing For Aadhaar

The question of whether or not privacy is a fundamental right arose during the hearings on the constitutionality of Aadhaar. The state argued that although a number of Supreme Court decisions had recognised the right to privacy, the Constitution does not guarantee such a fundamental right. Further, the state argued that since larger benches of the Court in M.P Sharma (8 judge bench) and Kharak Singh (6 judge bench), had refused to accept that the right to privacy was constitutionally protected subsequent SC judgments that accepted the right to privacy as a facet of Article 21 were contrary to the dicta laid down by the SC. [225] Sensing the need for a clarification on the status of the right to privacy, in July 2017, a five-judge bench was constituted which decided to refer the question of the right to privacy to an even larger bench of nine judges.[226] The government’s contention on the right to privacy was a consequential delaying tactic because until this question could be decided, the larger constitutional challenge to Aadhaar could not be heard by the Supreme Court.[227]

The delay in forming a constitutional bench to deliberate on the right to privacy, allowed the UPA-II to create legitimacy for the Aadhaar scheme by moving the UIDAI under the DeitY and revising the Allocation of Business Rules. This enabled the government to further subsidise the costs for enrollment and work with public and private institutions like the TRAI, RBI and NPCI to expand the use of Aadhaar.

On 3 March 2016, the **Aadhaar** (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) **Act 2016,**[228] was passed as a Money Bill. [229] The money bill route was taken[230] to stifle debate and bypass the upper house where a previous attempt to legislate Aadhaar had been defeated.[231]

The Aadhaar Act converted the private consortium of UIDAI into a statutory entity under the MeitY and legalized the collection, organization and sharing of demographic and biometric information of residents. It grants the government powers to seek Aadhaar as a proof of identification for availing any subsidy/benefit expenditure on which are incurred from the Consolidated Fund of India or Consolidated Fund of State. Clause 57 expands the use of the Aadhaar beyond the state to “any body corporate or person” for the purpose of complying with laws or “or any contract to this effect.” Under the law bureaucrats have the power to decide when and under what circumstances the information ought to be shared in the “national interest.” The court can direct UIDAI to share information, a right to be heard has been established for the UIDAI but not for the person whose data is being handed over.

The Act went into effect in September 2016, clarifying the state's intent to back private companies using Aadhaar, irrespective of the ongoing legal and political opposition to the identity scheme. Its uninterrupted passage got politicians, constitutional experts and rights activists worried and several petitions challenging the legality of the Aadhaar Act were filed almost immediately and clubbed with the original set of cases.

In March 2017, the government mandated Aadhaar be linked to Personal Account Number (PAN) to file income tax returns (ITRs) and to allow the PAN to remain valid.[232] The government did not explain its reasons at the time, and even subsequently it has failed to make public any information on the decision to introduce Aadhaar-PAN linkage. [233] The SC upheld the linking of Aadhaar-PAN but stayed the operation of consequence for those people who did not already possess Aadhaar. The bench also made it clear that the Aadhaar-PAN linkage decision was not the final one pending the right to privacy case. As an interim measure, in December 2017, the SC passed an order extending all the Aadhaar-linking deadlines.

Right to Privacy and Constitutionality of Aadhaar

The right to privacy hearings started in July and went on for six days over three weeks and on 24 August, 2017, the Supreme Court in Justice K.S. Puttaswamy vs Union of India passed a historic judgment affirming the constitutional right to privacy. In six separate opinions the nine-judges unanimously declared privacy to be an inalienable, inherent basic fundamental right that can be located under Article 21 and other provisions of the fundamental rights chapter of the Constitution. However, like most other fundamental rights, the right to privacy is not an"absolute right" and is subject to the satisfaction of certain tests and benchmarks and a person's privacy interests can be overridden by competing state and individual interests.

It is important to note that only the majority opinion in a judgment i.e. signed by a total of five or more judges, is binding on future cases. The plurality opinion, written by Justice Chandrachud on behalf of four judges,[234] does not constitute the majority and along with the concurring opinions of the remaining five judges [235] does not constitute 'precedent' for future cases. However, the privacy judgment was critical for the adjudication of the constitutionality of Aadhaar.

The Aadhaar hearing went on from January-May 2018 and apart from the state, the UIDAI and several state governments, the RBI and corporate interests intervened to defend the commercial potential of Aadhaar. In September 2018, the five-judge SC bench concluded that Aadhaar does not tend to create a surveillance state and upheld the constitutional validity of the Aadhaar Act. The SC limited the scope of the Aadhaar to welfare subsidies, benefits and services paid out of the Consolidated Funds of India.

The SC also deliberated on the constitutionality of Clause 57 which permitted use of Aadhaar authentication for establishing the identity of an individual by "private" entities; "pursuant to law or any contract to this effect" and for “any purpose” and "subject to the requirement of informed consent". Clause 57 was unanimously struck down as being ultra vires the Constitution on the grounds that the use of authentication by private entities is disproportionate because it enables commercial exploitation of biometric and demographic information.[236] Additionally, the mandatory linking of Aadhaar to eKYC by banks, telecom companies and fintech providers was struck down, as disproportionate and violative of the right to privacy.[237] Despite the SC ruling that identity may only be established by Aadhaar-authentication for a purpose authorised by law and not by contract, the private sector came together to build an ecosystem around Aadhaar.

Part 4. iSpirt and the Layers of India Stack

In this section I focus on the emergence of the India Stack label, and the design, institutions, technical features associated with its four layers: authenticating identity, providing valid documents, paying for transactions and sharing of data.

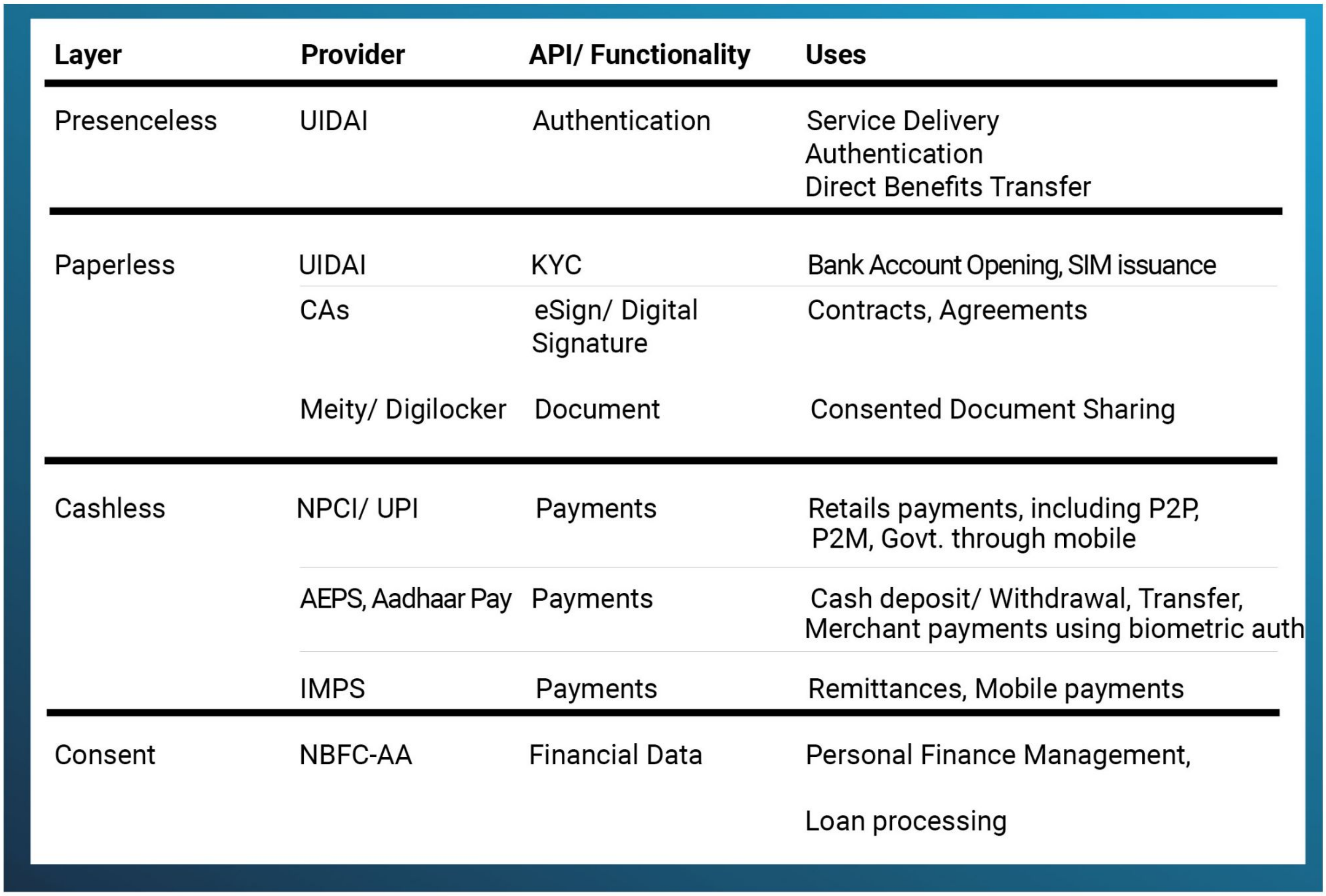
Recognizing the opportunity raised by the JAM trinity under the PMJDY, and the political backing for Aadhaar, the private sector jumped to leverage Aadhaar for their businesses. Amongst these was iSPIRT, the alliance of Indian software companies looking for opportunities to distinguish and scale their products and services. Given their role in growing the Indian software industry, iSpirt founders realised that their alliance was uniquely positioned to explore ways to embed and expand the use of Aadhaar and acquire government agencies or public institutions as clients. For the founders of the alliance, Aadhaar presented a “once in a lifetime opportunity” to solidify iSpirt's position as an intermediary between startups and the government, and expand its influence.

Between 2013-14 only a few companies in the iSpirt ecosystem were working with Aadhaar.[238] In 2015, iSpirt shifted its strategy and redirected its volunteers to build solutions for the expansion of Aadhaar and electronic payments systems in India. The NDA government encouraged iSpirt's involvement, because it aligned with technological self-reliance and its attempt to position India as a global technology hub. iSPIRT decided to collaborate with the public and private organisations like the UIDAI, the RBI, and the NPCI to build a “tech spine” or “technical scaffolding around Aadhaar", under the label of 'India Stack'.

The concept of a "stack" is used in software production, and refers to a specific hierarchical assemblage of hardware, network, protocol and software required to operate an application. In the same vein, "India Stack" is the moniker assigned to "a unified software platform" that “combines a set of Application Programming Interfaces (APIs) that enable autonomously run software programs to interoperate with one another.”[239]

India Stack APIs or programmable interfaces operate across three technology “layers” or processes that are essential to operating in the digital economy.[240] Initially, APIs were limited to provide “presenceless” identity authentication, “paperless” documents, and “cashless” payments.[241] As the use of solutions under the presensceless, paperless and cashless layers increased and the amount of data generated through these layers expanded, a fourth layer, “consent” was added.

The use of “stack” as a heuristic enabled seemingly disparate digital functions, platforms and services to be juxtaposed in a meaningful way by iSpirt. The APIs, software, networks and platforms were originally conceived to enable both government and private developers to “plug and play” Aadhaar for various functions, interact with systems and build applications. Today, the label is used to refer to a collection of disparate technology products or services and is described as "a set of open APIs and digital public goods that aim to unlock the economic primitives of identity, data, and payments at population scale."[242] India Stack APIs or "solutions" are described as “a unique convergence of government, technology and regulatory frameworks" and referred to as a "collection of digital goods connected to each other"[243] and "digital infrastructure as public goods".[244]



Layer	Provider	API/ Functionality	Uses
Presenceless	UIDAI	Authentication	Service Delivery Authentication Direct Benefits Transfer
Paperless	UIDAI	KYC	Bank Account Opening, SIM issuance
	CAs	eSign/ Digital Signature	Contracts, Agreements
	Meity/ Digilocker	Document	Consented Document Sharing
Cashless	NPCI/ UPI	Payments	Retails payments, including P2P, P2M, Govt. through mobile
	AEPS, Aadhaar Pay	Payments	Cash deposit/ Withdrawal, Transfer, Merchant payments using biometric auth
	IMPS	Payments	Remittances, Mobile payments
Consent	NBFC-AA	Financial Data	Personal Finance Management, Loan processing

Table 1. India Stack APIs[245]

Presenceless Layer: Expansion of Aadhaar; eSign

In the "presenceless" layer a digital identity linked to one or more digital identifiers would serve to authenticate identity. Aadhaar was already in place as the foundational layer of the India Stack. The UIDAI and iSPIRT collaborated on developing Aadhaar linked e-auth and e-KYC services to allow businesses to integrate Aadhaar into their products and services.

iSpirt and the UIDAI collaborated to enable Aadhaar to be linked to document signing. The prior process for electronic signatures required citizens to obtain a Digital Signature Certificate (DSC) from a Certifying Authority (CA) licensed by the Controller of Certifying Authorities (CCA). Before a CA can issue a Digital Signature Certificate (DSC) it must verify the identity and address of the signer. The process of verification of identity & address involves in-person physical presence and paper based documents, as well as the issuance of hardware cryptographic tokens to store the private key used for creating the electronic signature.

To simplify this process, an online electronic signature service, eSign, was introduced by the CCA.[246] eSign enables an Aadhaar holder to digitally sign documents such as contracts and agreements within seconds. The authentication of the eSign is facilitated through UIDAI's e-KYC service. iSpirt helped develop technology specifications for eSign which is maintained by the Ministry of Communications and Information Technology.

Paperless Layer: Digital Locker

The “paperless” layer is aimed at eliminating the use of physical documents. In this layer Aadhaar was linked to the storage of documents. In February 2015, MeitY rolled out the beta version of DigiLocker[247] to enable authorised organisations and citizens to issue, verify, store access, and share electronic copies of documents like identity cards, PAN card, vehicle registration, ration card, VoterID, passport, mark sheets and degree certificates.

The DigiLocker enables authorised service providers or issuers of documents like state, central departments, agencies or corporates to issue documents in an electronic format directly to a citizen's 'digital document wallet'. DigiLocker also serves as a platform that brings together holders of documents (citizens), issuers of documents (government departments and bodies) and requesters of documents (public agencies providing services) and enables consent-based sharing of verified electronic documents between them.

Technical Components of DigiLocker

The DigiLocker Portal is a web and mobile based portal that provides access to repositories and access gateway for citizens, issuers, and requesters to issue and access digitally signed or authenticated electronic records in a uniform way in real-time. The Digital Locker Directory provides information about the identity and registration facility for issuers, requesters, locker providers, repository providers and gateway providers. It also covers the details of standards, procedures and electronic workflow to request, approve, and publish new ID for new issuers, gateways and repositories.

Citizens grant access to their electronic records by providing a unique document Unique Resource Identifier (URI) to organisations registered with DigiLocker. Issuers can choose to maintain their own cloud-based repository or use a repository from an authorised repository service provider to store electronic records. Issuers also use APIs to notify subscribers about their records stored in the issuer repository and to allow the subscriber to query the issuer repository about or access a specific record.

Entities requesting documents use the DigiLocker portal to access and use authorised gateway providers to access documents stored across repositories. It accesses government issued digital documents stored in a citizens DigiLocker based on the URI and by taking consent from the citizen. iSpirt helped develop the APIs and the DigiLocker portal.[248]

Institutional Components of DigiLocker

The Digital Locker Service Provider (DLSP) must seek a license from the Controller of Digital Locker Authority (DLA) to operate.

Citizens can register on the DigiLocker portal with their Aadhaar to use the services of the licensed or empanelled DLSP for the purpose of accessing locker, gateways and repository services. Citizens can scan and upload copies of legacy documents, and electronically sign them using the eSign service to store it in the DigiLocker.

Authorised issuers of documents like state and central departments, agencies or body corporates register with the Digital Locker Directory. Registered issuers are authorised to issue new digital records in the prescribed format and must provide older digitized records in a 'verifiable, shareable, accessible and printable' format. Issuers are required to preserve and retain standardised digitally signed and/ or digitized electronic records issued by them in repositories.

The entity requesting access to documents through DigiLocker must register with the Digital Locker directory to access documents uploaded by the subscriber. Issuers can consent to any other Digital Locker service provider to gain access to documents maintained under its issuer repository. The issuer and requestor of documents are required to seek consent before depositing or accessing electronic documents of citizens.

Adoption of DigiLocker

On 1 July 2016, Digilocker was officially launched by PM Modi, as a flagship initiative under the Digital India programme and created for the 'Digital Empowerment' of citizens. The Digital Locker Rules were issued in 2016 directing government and other service providers to provide a Digital Locker system for “preservation and retention of machine readable, printable, shareable, verifiable and secure electronic records of government issued documents.”[249]

The Rules mandate that all the “infrastructure associated with all functions of Digital Locker system as well as maintenance of directories containing information about the status of Digital Locker system shall be installed at any location within India.” The Rules require Digital Locker service providers to enable subscribers to port their Digital Locker account to any other Digital Locker service provider". Service providers are required to “observe data retention and data migration guidelines as notified by DeitY” and submit to an annual audit by an independent auditor the report of which should be submitted to the government and the Digital Locker Authority within four weeks.

Currently the service is free but the Rules note the possibility of service providers charging subscribers or users the structure of which will be decided by the government or the Digital Locker Authority. On 8 February 2017, the Digital Locker Rules were amended to recognise that issuing certificates or documents in the Digital Locker System and accepting certificates or documents shared from Digital Locker Account was at par with Physical Documents.[250]The amendment also mandated Digital Locker service providers to appoint grievance officers for dispute resolution.

As of 2023, 5.62 billion documents have been issued through the DigiLocker and 2311 and 166 organisations have registered as issuers and requestors respectively. DigiLocker claims it has 149.97 million users. The top documents accessed through the DigiLocker includes Aadhaar Card, PAN Verification Record, Insurance Policy - Two Wheeler, Ration Card, and Registration of Vehicles. Top issuer of documents include UIDAI, Ministry of Road Transport and Highways, New India Assurance Co. Ltd., Income Tax Department, and the Life Insurance Corporation of India.

Cashless Layer: Unified Payments Interface (UPI)

The "cashless" layer of India Stack was conceived by various players in the financial industry, who for different reasons wanted to integrate Aadhaar authentication with digital payments. The UIDAI hoped that integrating Aadhaar with digital payments would strengthen its acceptance as an identity for the digital economy. The RBI and NPCI were pushing adoption of digital payments through the financial inclusion and delivery of government subsidies. In this context, the RBI NPCI and UIDAI had been collaborating to develop and integrate several Aadhaar-linked payments products in government programmes and schemes. Working on these projects, these institutions had realized that the combination of Aadhaar and digital payments had "explosive potential once network effects come into play."[251] iSpirt, which was looking for ways to distinguish itself from other service providers in the market, joined forces with these institutions to expand its portfolio of India-specific software products or services into the banking and financial sector.

Technology led to digital payments emerging as a distinct industry, dominated by fintech companies. To serve their customers fintech companies connect to, and access transaction data from different banking systems. They were pushing for the development of interoperable banking solutions but the idea faced resistance from banks which viewed fintech and startups as competition that may take away customers.

With the cashless layer the NPCI saw a way to integrate banks into the development of digital payment instruments and products, enabling them to compete with fintech companies. Fintech companies supported the development of the cashless layer as it provided a way to open up the banking sector and enable them to develop innovative products.

***The cashless layer* became the site for collaboration between both groups, as replacing the use of cash was the only way for either to grow.**

Turning financial transactions into digital transactions, would allow both traditional and new financial service providers to charge nominal fees on every single transaction. It would also create a trail of data on the income and spending patterns of customers which could be repurposed to sustain new services and business models.

Unified Payments Interface (UPI)

In 2014, a Technical Committee established by the RBI for the modernisation of banking infrastructure recommended public-private partnership for building a “common mobile application which will enable the use of encrypted SMS messages for banking transactions.” [252] The NPCI decided to collaborate with iSpirt to build this application under the cashless layer of India Stack, labeling it Unified Payment Interface (UPI).

The architects of UPI settled on creating this application layer by abstracting the payments on top of the existing IMPS system which is owned and operated by the NPCI. They hoped that this “IMPS on steroids" approach would have a two-fold effect. It would simplify the transaction process, allowing Indian consumers to link more than one bank account in a single mobile app, and transfer funds without IFSC code or account number. It would allow banks to acquire any bank’s customers[253]while also enabling them to communicate and exchange transaction data with non-banking firms, paving the way for new players in the digital payments market.[254]

The UPI would function as both a funds transfer enabling real-time movement of funds and a merchant payment system in which settlement happens on a deferred net basis. The payment system operator NPCI and banks, PSP mutually decide systems and processes to address the settlement risks.

Technical Components of UPI

To transfer funds or make payments using UPI, users need a smartphone, an Internet connection, and download a UPI-enabled mobile payment app. The app allows users to register their mobile number and bank account to generate a unique UPI Id and set up a four to six digit password for transactions. The mobile and bank linked UPI Id serves an accessible virtual id or payment address, simplifying the transaction process.

Payments on UPI can be made using the recipient's mobile number, UPI Id, bank account number and IFSC code, or by scanning the recipient's QR code. Payments are directly debited from the bank account (s) linked to the UPI Id but consumers also have the option to use wallets to make payments on UPI. UPI also allows users to request a payment from another UPI user. The user credentials and transaction data collected by the app is encrypted and stored in a centralised payment data repository or the UPI common library. Juspay as a vendor to NPCI built the UPI Common Library which is embedded in each app. The technology and the server code for the UPI infrastructure was built by a private Indian company called RS Software. [255] Once developed NPCI filed a patent application for the technology.[256]

UPI is also linked to Aadhaar via the BHIM Aadhaar Pay feature, a point of sale payment solution wrapped on AePS. BHIM Aadhaar Pay, allows merchants to use biometric authentication to accept digital payments from customers with Aadhaar linked bank accounts. To use this feature merchants need to link their Aadhaar and bank account, download the Android BHIM app and have access to a certified biometric scanner linking it to the phone, kiosk, tablet or other payment device. UPI had included a Pay-to-Aadhaar feature to enable an Aadhaar based remittance system. This was discontinued after evidence of misuse of the feature with leaked Aadhaar numbers was demonstrated by hackers.

Institutional Components of UPI

Processing digital transactions through UPI involves a number of parties. Payment Service Providers (PSP) are RBI-authorized entities that provide a UPI-enabled app and verify the UPI Id of the sender and receiver to authorize each transaction. PSPs can be both banks and non-banks or fintech startups. in Banks provide backend services and in most cases also function as PSPs. In each UPI transaction, at least seven parties are involved: the customer and their bank (issuing bank), the merchant and their bank (acquirer bank), PSP apps of both the sender and the receiver, and the NPCI.[257]

Adoption of UPI and RuPay

In February 2016, the Ministry of Finance released guidelines for government ministries, departments and their public sector undertakings to replace the use of cash, either in government transactions or in regular commerce, with digital transactions over a period of time.[258] The Ministry called for policy interventions to restrict use of cash to 'specific circumstances, for clearly stated reasons' and mandate digital payments for transactions beyond a prescribed threshold. The guidelines proposed several measures to facilitate digital payments such as investments in digital payment acceptance infrastructure for commercial services, the creation of a single unified portal for government transactions and reducing barriers for pre-paid instruments and mobile banking. In March 2016, the government issued action-points based on the guidelines and sought implementation timelines from all government bodies.[259]

In April 2016, the RBI approved the roll-out of UPI. Following a closed - environment test with twenty - one banks, NPCI allowed all member banks to upload their UPI integrated apps on app stores and began promoting them.[260] Simultaneously, the NPCI began pushing for UPI's adoption by non-member and public sector banks, promoting UPI under the India Stack umbrella. The RBI and NPCI decided not to charge customers for payments made over UPI. It set the daily transfer limit for UPI users at INR 1 lakh and at INR 5 lakh for bill payments and merchants. Banks were free to set their own UPI transfer limits on a daily, weekly or per month basis.

In June 2016, the RBI released its vision and plan for building a payment and settlement systems for a 'less-cash' India through responsive regulation, robust infrastructure, effective supervision and customer centricity.[261] In August 2016, the Ministry of Finance constituted a committee on digital payments under the Chairmanship of Ratan P. Watal,[262] Principal Advisor, NITI Aayog (Watal committee). The Watal committee was tasked with identifying market failures, regulatory bottlenecks, and measures to incentivize transactions through cards and digital means including the leveraging of Aadhaar for authentication, introduction of a payment gateway, setting up of a centralized KYC registry and using payments history to provide access to credit.

On 8 November 2016, the NDA government demonetized 1,000 and 500 banknotes leading to an acute shortage of cash in the economy. The timing and reasoning for demonetisation may have been shaped by political reasons and the schedule of the Assembly elections, but the move towards a cashless economy was already underway, as highlighted above. While debit and credit cards including NPCI's RuPay were available, their access was limited to the affluent and the use of cards at PoS terminals was limited. Increase in penetration of low-cost smartphones, the low cost of 4G data and rise in e-commerce had created a massive user base that was ready to adopt digital payments. As cash became scarce, consumers, banks and merchants made a beeline for digital payments solutions but had few options.

Member banks of NPCI which had created their own UPI-enabled apps had a first movers' advantage in the UPI payment space. Following demonetization, there was a spurt in digital payments across the country and both the volume and amount of money transacted through cards and UPI saw manifold increase. To cater to the massive demand for digital payments following demonetisation, the NPCI wanted a UPI-based transaction app for itself and turned to iSPIRT volunteers involved in building UPI to create Bharat Interface for Money (BHIM) app.[263] The BHIM app is available for both Android or iOS operating systems and is interoperable with other third-party UPI apps.

Between 2016-2019 the regulatory regime for digital payments was being defined through ad-hoc notifications and circulars of the RBI and the NPCI, creating uncertainty for the payments market. As the guidelines and approach became clearer, new players began to emerge. Despite their advantages banks were unable to utilize their dominance on UPI as an opportunity for growth.[264] Most of the bank-led UPI apps were treated as another avenue for banking and were not user-friendly. As a result of the government and the NPCI promoting and marketing BHIM-UPI as the 'official' UPI-app and a cashback programme backed by the MEITy, the BHIM App soon dominated UPI.[265] BHIM App is not the only government backed payment service, it is the one where the government acting as a player, the regulator and the venture capitalist in the market is most visible.[266]

The Move to Zero MDR

In December 2016, the Watal committee released its report on strengthening the digital payment ecosystem.[267] The committee recommended several structural reforms such as updating the PSS Act, strengthening the BPSS and creating an independent Payments Regulatory Board (PRB). The report called for minimal regulatory and policy interventions focused upon removal of entry barriers, and ensuring greater competition in the markets. These included ensuring access to payment systems for non-bank PSPs and interoperability of payments between bank and non-banks as well as within non-banks. It recommended the government to remove all charges, fund discounts or cashbacks, relax authentication and taxation standards for digital payments and reduce custom duties on payments equipment. With regard to pricing the committee recommended that the setting of Merchant Discount Rate (MDR) should be market driven; however, interchange fees and differential MDR caps may be regulated on an evidence based approach.

After demonetisation, most of the Watal committee's recommendations were implemented.[268] The government funded discounts and cashbacks for consumers and merchants to incentivise them to use UPI and RuPay cards were extended to farmer credit holders.[269] provisioning of PoS infrastructure and devices by public sector and private banks was subsidized resulting in a reduction of costs of PoS devices from INR 5000 to INR 10000 to INR 1500-7000. For comparison, setting up an ATM required investment of INR 1-5 lakhs per machine and the paying real-estate costs. As a result of these interventions, the availability of PoS devices increased by 95 percent to 22 lakhs and the use of cards at PoS more than doubled from 131 million in 2016 to 265 million in 2017.[270]

Apart from subsidizing payment acceptance infrastructure, the government intervened in the pricing of digital payments. Banks and PSPs bear the costs and risks for processing, accepting, and authorizing digital transactions through cards, prepaid payment instruments (PPIs) or systems like UPI which are offset to an extent by charging transaction fees. In a funds transfer payment system, the fixed charges are levied as an add-on remittance amount and recovered from the originator of the payment. In a merchant payment system, the transaction charge is recovered from the final recipient of money (merchant) and varies depending on the payment method. For e.g. digital transactions are charged higher than transactions at physical PoS terminals.

To accept payments from customers, merchants or recipients of funds pay a MDR fee to their bank (acquirer bank) which is calculated as a percentage of the transaction value. A proportion of MDR charges, called interchange fees, is used by the acquirer banks to ensure acceptance of its payment mode. The interchange fee acts as income for issuing banks, network operators, PSPs, and other intermediaries. Ideally, both MDR and interchange fees should be determined by the market. For e.g. digital wallets charge 1-2 percent of total transaction value as MDR plus and an additional Goods and Services Tax (GST) as transaction charges.

To manage the risks of real-time payment and deferred settlement, the NPCI has put in place arrangements like maintaining settlement guarantee funds and loss sharing arrangements among banks in case of default by a member. Banks and other entities like PSPs contribute to such funds as costs of participating in the UPI or IMPS network. As of June 2022, NPCI had total settlement guarantee funds of INR 9073 crore and lines of credit worth INR 7779 crore from various banks to meet any shortfall during the settlement of transactions across the product segments. [271] To recover operational and settlement risk management costs the consumer is charged by their bank (acquirer bank) and NPCI charges the acquirer bank a transaction fee typically in the range of INR 2.5-15 (depending on amount) for transfer of funds over IMPS. Stakeholders in the UPI ecosystem incurred a cost of INR 2 for processing an average person to merchant (P2M) transaction of INR 800. [272] UPI transactions of over INR 100 attract an MDR of 0.3 percent (MDR capped at INR 100).

Initially, card payment system operators like VISA and Matercard were setting the MDR at the same level for debit and credit cards. The distribution of interchange between the acquirer bank and the intermediary was based on contracts. One of the main friction points in the adoption of debit or credit cards was high charges associated with their use for cash withdrawal at ATMs and their acceptance at PoS terminals. After launching RuPay, the RBI decided to prescribe the maximum MDR rate rather than a fixed rate to enable market discovery of ideal rates based on the cost benefit analysis of various stakeholders. With effect from September 2012, the maximum MDR for debit card transactions was set at 0.75 percent of transaction value for transactions up to INR 2,000, and at 1 percent for those above INR 2,000. [273] This was in effect till December 2016.

Following demonetisation, the government wanted to encourage acceptance of RuPay debit cards for small value merchant payments. In January, 2017 the maximum MDR rate on debit cards was lowered to 0.25 percent of transaction value for transactions up to INR 1,000, and 0.5 percent for those above INR 1,000 and up to INR 2,000. [274] Despite slashing rates, the use of debit cards at ATMs dipped from 757 million in 2016 to 716 million in 2017.

The government responded by hiking the overall MDR rate for debit cards and introducing a differentiated MDR regime based on the turnover of merchants. With effect from January 2018, the MDR on debit cards transactions was set at a maximum of 0.4 percent (MDR cap of INR 200 per transaction) for small merchants with turnover upto INR 2 million and 0.9 percent for other merchants (MDR cap of INR 1000 per transaction). The increase in MDR rates was opposed by Retailers Association of India (RAI) which claimed the move was "absolutely against the Digital India thought process."[275] The hike impacted the margins of all businesses with a turnover of more than INR 20 lakhs that process large volumes of small denomination transactions like Indian railways, ecommerce and cab or food aggregator companies. The RBI defended its stance by claiming MDR charges were necessary for banks to recover costs and the differentiated MDR regime safeguarded the interests of smaller merchants. To ensure customers and merchants were not charged, the government announced that it will bear the costs of MDR charges for all debit card, BHIM UPI and Aadhaar Pay transactions up to INR 2000 for a period of two years.[276]

In January 2019, RBI formed a committee headed by Nilekani to identify the gaps in the digital payments.[277] Unlike the Watal committee which had recommended pricing should be market-driven, the Nilekani committee believes market-based MDR and interchange fees were not working and had led to an "acute paucity of acquisition infrastructure in the country." It called for regulatory interventions on pricing including establishing an RBI standing committee to review the MDR and interchange rates periodically to benchmark rates. To ensure "a level playing field in the market between issuer and acquirer" the committee recommended reducing the interchange fee card payments by 0.15 percent. In May, 2019 based on the Nilekani committee's recommendations the RBI published its Payment Systems Vision 2021.[278] The RBI moved away from its approach of minimal intervention in the pricing of charges and adopted a pricing approach aimed at "recovery of marginal costs" and "migrating to a low margin-high volume regime."

In July 2019, the Finance Minister in her Budget Speech 2019 announced a Tax-Deducted-at-source (TDS) of 2 percent would be levied on cash withdrawal exceeding INR 1 crore (USD10 million) and removal of the MDR charges applicable on payments made through RuPay, BHIM-UPI and UPI QR Code. The withdrawal of MDR was implemented by way of amendments to various legislation. Section 269SU and Section 271DB of the Finance Act mandates business establishments with annual revenue of over 500 million to "provide facilities for accepting payment through prescribed electronic modes" and businesses would be penalized INR 5000 per day for not enabling digital payments. Section 10A in the PSS Act provides "that no bank or system provider shall impose a charge on a payer, or a beneficiary receiving payment" through prescribed electronic modes under the Finance Act. UPI and RuPay were notified as prescribed payment modes under the Finance Act through the Income Tax Rules and the zero-MDR regime came into effect on 1 January, 2020.[279] Subsequently, the government announced it will bear the costs of operationalizing zero-MDR which is estimated to be INR 8000 crores by the Payments Council of India (PCI).[280]

The Consent Layer: DEPA, Account Aggregator

The development of the consent layer of India Stack has been shaped by the case on the fundamental right to privacy, which emerged from the Aadhaar hearings as well as the many efforts to create a data protection law in India. Consent is the bedrock of the third layer, and the emphasis on consent has enabled disparate initiatives and approaches for sharing of data to be combined as part of the consent layer. However, consent is being used to enable sharing of personal and non-personal data instead of furthering other principles like ensuring limited data collection, data protection or data portability.

The consent layer of India Stack emerged in the context of account aggregation in the financial sector. A critical function of financial systems is coordination of those seeking loans and those offering funds to find each other and provide credible assurances that loans are going to be repaid. The financial data of consumers like savings and current deposits, equity, mutual funds, loans, credit cards, pension, provident fund, and income tax returns are spread across financial institutions, government bodies and other private or public service providers.

Traditional and new financial institutions like banks, investment firms, fintech companies view the fragmented nature of financial data and the lack of accessibility mechanisms as barriers to reducing costs of operations, creating better products and improving the delivery of financial services. Financial service providers seeking organised access to financial data were incentivised to pursue aggregation of consumer financial data. From the perspective of policymakers, aggregating financial data would improve the government's decision-making on providing financial services and credit for earlier underserved and unserved segments and help with achieving the goal of financial inclusion.

Design of Account Aggregator

The creation of an “account aggregation facility” was first discussed in 2014 by the Financial Stability and Development Council (FSDC)[281] which established an Inter Regulatory Technical Group (IRTG) to create standards and protocols for setting up a one-stop portal to enable individuals to access their financial data spread across various institutions. Recognizing that account aggregation would require financial institutions to bring in technical providers to provide specialist expertise and reduce operational costs, the RBI issued guidelines to manage the risks of outsourcing operations to third-party providers.[282]

In July 2015, the RBI noted that the financial inclusion agenda had assumed critical importance under PM Modi and following the efforts for integrating the JAM trinity in the digital economy. It proposed to recommence the Financial Inclusion Advisory Committee (FIAC) and develop a blueprint "identifying ways to integrate resources available with all financial institutions" to take the financial inclusion agenda forward. The RBI requested the government, all regulators, self-regulatory and research organisations in the financial sector, the UIDAI, and the NPCI to nominate members to the FIAC. In the same press release the RBI announced it will put in place a regulatory framework to "allow a new kind of Non-Banking Finance Company (NBFC) which would act as an account aggregator to enable the common man to see all his accounts across financial institutions in a common format." [283]

In March 2016 the RBI initiated consultations exploring a regulatory framework for a new kind of NBFC which could act as an account aggregator (AA).[284] The scope of the AA had been expanded from enabling consumers to view information held in accounts across financial institutions to "collecting and providing the information of customers' financial assets in a consolidated, organized and retrievable manner to the customer or any other person as per the instructions of the customer."[285] Only companies licensed by the RBI or other financial sector regulators the Securities and Exchanges Board of India (SEBI), Insurance Regulatory and Development Agency (IRDA) and Provident Fund Regulatory and Development Agency (PFRDA) — could undertake account aggregation.

Companies that register as an AA are prohibited from undertaking "any other business" except an "entirely Information Technology (IT) driven" aggregation business that is "scalable to cover any other financial assets or financial service provider." The AA can charge for its services which must be provided "under specific application by the customer" and be "backed by appropriate agreements/ authorisations between the AA, the customer and the financial service providers." The AA cannot "store financial asset related customer information pulled from the financial service providers" or use it for any other purpose like supporting "transactions in financial assets." The draft framework mandated AA to put in place robust mechanisms for customer identification, authentication of authorization for data sharing, and customer grievances redressal.

On 2 September, 2016 the RBI issued directions for the registration and operation of the Account Aggregator (AA) institutionalising the framework for aggregation and sharing of financial data in India.[286] The AA framework is part of the India Stack project and extends the reach of iSPIRT from payments into credit, personal finance, wealth management, and insurance. As noted by Nilekani, "Now you can think of an end-to-end credit cycle that's entirely digital...from origination and underwriting to disbursement and repayment. That's possible because of UPI, Aadhaar, and account aggregation."[287]

Technical & Institutional Components of Account Aggregator

The AA is an intermediary that retrieves and collects financial information of consumers from Financial Information Providers (FIPs) holding it. It consolidates this financial information and makes it available for access by consumers or Financial Information Users (FIUs) i.e. entities seeking access to consumer's data in exchange for services. The AA performs these functions under a contract, in exchange for a fee and "based on the customer's explicit consent." An AA is prohibited from using "the services of a third party service provider for undertaking the business of account aggregation." It is prohibited from accessing, storing or using financial data for any other purpose other than that specified by the consumer and financial data can only be shared with regulated financial entities.

The directions introduced a standardised consent artefact or a machine-readable electronic document which specifies all the entities that are involved in the data sharing transaction, describes the type of data that is being accessed, the permissions associated with each of them and the purpose of data access. The consent artefact must include signatures of all involved parties for logging of consent, and a URL or other address to log data access, use and flows. It must also enable customers to revoke consent for data access and further use of consolidated financial data. The AA consent artefact was developed and designed by the Reserve Bank Information Technology Pvt. Ltd (ReBIT) - a wholly-owned unit of RBI - in collaboration with iSpirt. ReBIT owns the technology standard for real-time aggregation of financial information in India.

In January 2019, the RBI granted[288] in-principle Non-Banking Financial CompanyAccount Aggregator (NFBC-AA) licence to six companies. One of them was NeSL Asset Data Limited (NADL) a subsidiary of the private information utility company National eGovernance Services Limited (NeSL).[289] It also implemented a regulatory sandbox to test out the framework in a live environment. By April 2019 seven AAs had gone into a closed user group testing which ran for three months.[290]

A High-level Committee on digital payments headed by Nilekani came out in support of the RBI's regulatory sandbox for the AA ecosystem, recommending that it be used "to test ideas on how to serve customers who are currently hard to serve."[291] The committee called on regulators to facilitate the creation of a Self-Regulatory Organization (SRO) for the recently licensed NBFC Account Aggregators" which "can serve as a blueprint for more SROs that may be created later in the area of digital payments."[292]

Representatives from the financial services industry came together to create a non-profit member driven industry alliance called Sahamati as a SRO for the AA ecosystem.[293] Siddharth Shetty, a Fellow of the iSPIRT Foundation, co-founded Sahamiti with the aim of "empowering Indians with their data for a better financial future."[294] Sahamati - which roughly translates into agreement or consent - is an appropriate choice of name for the alliance. Much of the alliance's work is expected to be focused on supporting implementation and adoption of a standardised electronic artefact for obtaining, submitting, managing and revoking the customer's consent.

By late 2019, the first NBFC-AA operating licence was issued and the RBI had issued technical specifications for all participants of the account aggregator ecosystem.[295] The AA framework was limited to the financial sector but revealed the possibilities of sharing of data across domains and sectors.

Institutionalising Consent: Standards and Agents

The government had laid down the principles and software requirements for the sharing of data collected by the government in public interest under the NDSAP and Open APIs policies.[296] Building on the approach laid down under the earlier policies, the MeitY proposed creating an API based centralised consent 'artefact' for "data to be electronically and securely shared with service providers on an as-needed basis, while maintaining traceability to ensure that the data trails can be audited in the future."[297]

In March 2017, MeitY released the Electronic Consent Framework covering the design principles, the technical format for data requests, and specifying the terms of data access and use.[298] The *artefact* would allow logging of both consent and data flows is deemed to be necessary as "collecting and sharing user data" through "a paperless, fully electronic, and high trust way" "is a key requirement for ensuring that the interaction between a user and the service provider can be consummated seamlessly."[299]

Situating the consent artefact within the consent layer of India Stack, MeitY notes "just as Aadhaar e-KYC, eSign, and Digital Locker provides digital equivalents of the corresponding physical paper based process", the electronic consent is the digital equivalent of "a physical letter of permission given by the user which, when presented, allows the data provider to share information regarding the user with a data consumer, for a particular purpose." The electronic consent framework was adopted by financial regulators the RBI, SEBI, IRDAI, and PFRDA for implementation of the AA model.

The AA ecosystem for the financial sector and MeitY's electronic consent framework was being created in parallel to other legislative and sectoral efforts for managing consent based data sharing. In November 2019, the Ministry of Health and Family Welfare released the National Digital Health Blueprint identifying consent managers as one of its building blocks.

In December 2019, the PDP Bill, emphasising consent and individual autonomy as the foundation for privacy and data protection, was introduced in Parliament. The PDP Bill aligned with the consent driven data sharing approach as it made it illegal for institutions to share personal data without consent. The data protection framework under the PDP Bill adopted a tripartite model for consent based-data sharing. Information providers collect and store the individual's data and are the original custodians of data. Information users are entities that need access to data of consumers to provide services.

Notably, the bill recognizes a "consent manager" as a data fiduciary "which enables a data principal to gain, withdraw, review and manage his consent through an accessible, transparent and interoperable platform." [300] Consent managers are third-party entities registered with the data protection authority and are "subject to technical, operational, financial and other conditions specified by regulations". They operationalize digital consent management through an interoperable technology framework such as the electronic consent framework established by MeitY. The PDP Bill was referred to a Parliamentary Standing Committee on 11 December 2019.

On 15 August 2020, Prime Minister Narendra Modi announced the Ayushman Bharat Digital Health Mission, which mandates the creation of a Health ID and a data-sharing framework for personal health records.[301] The Digital Mission recognizes consent managers to be one of the building blocks for the management of [302] electronic health records under the scheme. The Parliamentary Standing Committee in its report on the PDP Bill published on 16 December 2021 reinstated the concept of "consent managers" and recommended its insertion into the definition clause of the upcoming Data Protection Act.[303]

Design of Data Empowerment and Protection Architecture (DEPA)

On 5 May, 2019 iSpirt introduced a new approach, which it called “a paradigm shift in personal data management and processing,” the Data Empowerment and Protection Architecture (DEPA).[304] Work began on DEPA as far back as August 2017 and it was introduced as the consent layer of India Stack in May 2019. DEPA is a techno-legal framework that takes forward the idea that "encouraging and mandating organisations to seek the consent of the user" for the collection, sharing and use of personal data will “empower every Indian with control over their data” enabling them to derive value or benefits from their data. iSpirt announced that DEPA’s implementation was underway in the financial sector through the AA framework. The framework introduces data access fiduciaries to enable personal management of consent to “democratise access” and “enable the portability of trusted data between service providers.” DEPA is also expected to be rolled out in the telecom sector.

In August 2020, the National Institution for Transforming India (NITI) Aayog, India’s official think tank which replaced the Planning Commission, put out a discussion paper on the DEPA. The report describes DEPA as a “truly an ecosystem-wide, joint public-private effort for a new and improved data governance approach” which “combines public digital infrastructure and private market-led innovation.” The contributions of iSpirt, whose donors include fintech players like PhonePe and PayTM and individuals linked to iSpirt are noted in the report. DEPA's development has also been supported by several government ministries, sectoral regulators and key financial players including iSpirt, DICE India (a digital payment providers’ collective), CredAll (a consortium of lenders), and Sahamiti (AA industry alliance).[305] Nandan Nilekani and other individual thought leaders on financial inclusion, data, and privacy like Justice B.N. Srikrishna, Arundhati Bhattacharya, and Rahul Mathan are credited as the key players orchestrating the rollout of DEPA.[306]

Technical and Institutional Components of DEPA

DEPA operationalises the consent layer of India Stack by creating an evolvable, sector-agnostic, and overarching framework that covers regulatory, institutional, and technological aspects of electronic consent management for sharing and use of data. Consent-based data sharing under DEPA relies on the interaction between its technical components and the institutional arrangements required to facilitate these exchanges.

The basic building blocks of DEPA's technological architecture includes three *digital public goods:* MeitY's Electronic Consent Framework which provides the specification for consent artefact (to log consent and data flows),[307] data sharing API standards (to enable data exchanges), and sector specific data information standards.[308] DEPA is framed as a tool that empowers individuals to access socio-economically important digital services in a secure and privacy-preserving manner. Individuals extend control over their data by making decisions about what types of data can be shared, with whom, for what duration and purpose and communicating these decisions through the consent artefact that will be enabled through a new class of intermediaries or market players called consent managers.

The concept of consent managers was introduced in the PDP Bill that has since been withdrawn by the government. As per DEPA's formulation, consent managers are supposed to be 'data blind' by design, which means that they can only facilitate sharing of data on the basis of informed and meaningful consent without being able to see the data themselves. The DEPA framework proposes that consent managers should be entrusted with protecting individuals' data rights around privacy as unlike current data fiduciaries, who are interested in collecting surplus data, a consent manager can only access that data which the individual has decided to make available. The consent manager is also required to provide users with the option to revoke their consent, including towards parts of information mentioned in the consent artefact.[309]

Critically, by allowing a consent manager to charge a nominal fee to facilitate exchange of data, the DEPA framework hopes to align the economic incentives of consent managers with enforcing individual's data rights around portability. Financial Information Providers and Financial Information Users are entities who seek access to invividual's data and between whom data sharing can take place based on the consent of the individual.[310] The current design of DEPA provides for a principle of reciprocity of data use and data provision, which means that an entity can access and use data only if it also agrees to share data in the system.[311]

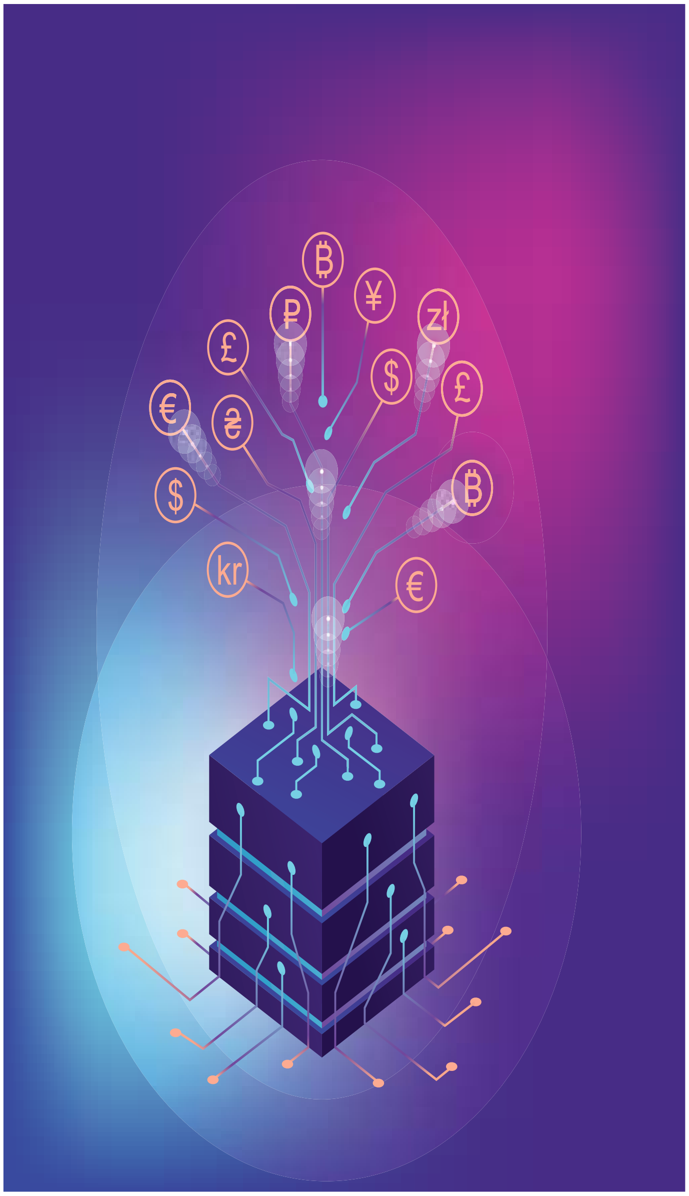
Implementation of DEPA & Adoption of Account Aggregator

Over the last few years, several government agencies have endorsed and implemented DEPA in various forms, sometimes by different names, and in a few cases even before the idea of DEPA was officially articulated in 2020. The NITI Aayog expects the adoption of DEPA to take place on a sector-by-sector basis with government departments and regulatory agencies setting the norms around how consent managers will operate in their domains. The PDP Bill had proposed that the DPA would have the authority to frame regulations to specify the technical, operational, financial and other conditions governing consent managers.

The implementation of DEPA was kickstarted in the financial sector with the AA framework and the NBFC-AA is the first application of DEPA's consent managers. Under the AA ecosystem's financial model, the FIU or the end consumer of data is charged a fee but not the FIP with whom the requested data resides. At the time of the release of NITI Aayog's paper on DEPA, three NBFCs had been granted operating licences by the RBI.[312] The release of NITI Aayog's paper accelerated the adoption of the AA ecosystem. Both Sahamiti and ReBIT took several steps to strengthen the AA ecosystem and align it with the technical and institutional components outlined under the DEPA.[313]

In August 2020, the Goods and Services Tax Department reached out to the RBI seeking to join the AA network. In March 2021, Sahamiti released a common legal framework for participants in the AA ecosystem. In July 2021 ReBIT tested the tech rails of the aggregator system with two AAs and six financial institutions.

On 1 October, 2019 the first NBFC-AA operating licence was issued and in November, the RBI issued technical specifications for all participants of the account aggregator ecosystem.[314] The AA system went live 2 September 2021, with four NBFC-AAs and eight major banks.[315] iSpirt, the driving force behind the AA system noted: “Just as UPI, NEFT, or IMPS are key financial utilities for secure flow of money, Account Aggregator is an urgent and powerful financial utility for the flow of data controlled by the individual.”[316] Speaking at the launch of AAs, the RBI Deputy Governor M Rajeshwar Rao said, “India is a world leader in building public digital infrastructure, and the Account Aggregator framework follows that tradition. AAs enable secure, consented data flows while protecting user privacy. In conjunction with other platforms like the Unified Payment Interface, Account Aggregator creates in India the most cutting edge digital financial infrastructure in the world.”[317]



Part 5. India Stack & Data Sovereignty

Data Sovereignty and Digital Identity (Presenceless Layer)

The development and expansion of Aadhaar in India's digital ecosystem, is part of India's data sovereignty strategy, and has been achieved by restricting access to the digital identity ecosystem while simultaneously enabling new concentration of power to accumulate data being created through the ecosystem.

Restricting Access to Digital Identity Market

National security was used to justify introducing real-time identity verification covering India's entire population. Initially, both the NDA and the UPA governments were focusing on smart cards for this purpose; however, terrorism and border conflicts during their terms shifted the focus to expanding the surveillance capabilities of the state. Consequently, the government decided to get involved in the provisioning and management of digital identity.

Aadhaar was made possible with the state creating legitimacy for the project and acting as an investor that subsidised costs of provision. It made enrollment, verification or usage free for users. Since the state lacked technological capacity, the UIDAI served as a critical intermediary that worked alongside the government to plan and design Aadhaar, in a vendor-customer mode. This arrangement enabled the state to outsource critical governance functions like planning and standards development to the UIDAI, while the UIDAI was able to use the state's authority to marshall resources for the development of Aadhaar.

The UIDAI handpicked multiple domestic and foreign biometric technology providers, vendors and agencies for the implementation of Aadhaar. The UIDAI and by extension the state exercises control over them through requests for proposals (RFPs), memorandums of understanding (MoUs) and monitoring and auditing their performance. The UIDAI also lays down a governance framework including processes and technical standards for security, interoperability, privacy and other issues associated with enrollment and authentication.

The UIDAI decided Aadhaar would be a unique number linked to biometrics that would enable ubiquitous online verification through the de-duplicated database. It decided that biometrics were the most reliable method for establishing ownership of an identity. It made this decision despite the concerns raised by its own Committee on Biometrics Standards about the efficacy of biometric de-duplication,[318] and the National Human Rights Commission flagging the dangerous ramifications for national security. The UIDAI assumed that biometrics were unique to an individual, and "valid for life" and thus not "vulnerable to forgery, falsification, theft, loss and other corruptions" and that even if they were faked, it would be caught during deduplication.[319]

Nothing in the UIDAI's rushed proof of concept report confirms that each Aadhaar number on the CIDR is unique or that biometric de-duplication could ever be achieved.[320] As noted by technology expert Sunil Abraham, the decision took biometrics, a form of *identity*, and repurposed it to present it as an *authentication technology.*[321] The architects of Aadhaar acknowledge that at the time of its introduction, the technology was not well-developed enough to enable real-time authentication; offline authentication has been a major driver of Aadhaar's adoption.[322] The use of biometrics for authentication in the same manner as a debit card pin is not secure, as biometric data is irrevocable, can be stolen easily and once stolen cannot be re-issued like a smart card."[323] Biometric-authentication also overlooks the larger issues of ageing, health and environmental factors, which can change biometrics, making the ones collected unusable or requiring frequent re-enrolment.

The welfare delivery system as the site for the deployment allowed the government to control the design of architecture, and involve local players in the development and implementation of the digital identity at scale; e.g., Wipro was hired as a consultant for the design of the digital identity. UIDAI was able to compel foreign biometric technology providers and other vendors to partner with Indian companies, enabling knowledge transfer, service customization, and compliance with restrictions on data transfers.

Restricting Access to Digital Identity Data

To ensure security of data and national security, the UIDAI decided to store sensitive biometric data in a centralised database. The creation of CIDR is a form of forced localization, a key tenet of India's data restriction strategy.

UIDAI laid down the conditions for access and sharing and in some cases used the biometric and demographic data of Indian citizens. Access to the application, audit logs, source code etc. or sharing of data was granted to authorised personnel, however the extent of access is unknown. Contrary to UIDAI's claims that private entities did not have access to unencrypted Aadhaar data, a Right to Information request revealed that *all three consortiums selected for providing various de-duplication services were given "full access" to classified biometric and demographic data "as part of [their] job."* [324] Biometric technology providers could collect, use, transfer, store and process the data for seven years and were required to transfer the "biometric template" to the UIDAI upon termination of their contract.

The UIDAI mandated Authentication User Agencies (AUAs) and Know-Your-Customer User Agencies (KUAs) to maintain logs for each Aadhaar-based transaction online for two years and offline for five years.[325] The UIDAI neither specifies encryption or safety standards for maintenance of logs nor has established mechanisms for verifying deletion of data. The UIDAI uses contracts to secure access to data for itself, but in the process restricts the right of citizens to seek deletion of data.

The state through Section 33 of the Aadhaar Act, has created a data access regime for itself. The UIDAI must share information pursuant to orders made by a district judge and share core biometrics (fingerprints or iris scans) and authentication information for the purposes of national security. During the constitutional challenges to Aadhaar, the Supreme Court upheld the state's right to access information held by the UIDAI in the interests of national security, but conceded to create a right to be heard for the person whose information is being sought along with the UIDAI.[326]The establishment of the right does not foreclose UIDAI's ability to run checks and share the results with law enforcement agencies. Aadhaar has proven vulnerable to criminal misuse[327] and as the misuse of Aadhaar grows, the demands from law enforcement agencies to use Aadhaar for criminal investigations and surveillance are likely to also increase.[328] Recently, the Punjab and Haryana High Court have passed orders requiring UIDAI to provide or share information involving fake Aadhaar cards.[329]

Securing Digital Public Infrastructure

Aadhaar is described as a 'digital public infrastructure' that provides a reliable digital identity, e-KYC service and Aadhaar authentication services to enhance security of online transactions. Ideological rationales for digital sovereignty always involve claims of improved security for citizens. However, UIDAI's record at securing the Aadhaar database and ecosystem has been abysmal, and its mismanagement has created new threat vectors.[330]

A recent audit report by the Controller and Auditor General of India (CAG report) reveals that for the first four years of its operations, Aadhaar numbers were issued without verifying personal documents submitted by residents.[331] The loopholes in the enrollment process impact the quality of data stored in the CIDR and have led to various vulnerabilities such as duplication, fake enrollments, and enrollments with unverified documents among others. Aadhaar numbers were issued to dogs, chairs, trees and even Hanuman, the hindu God. [332] The mechanism for the delivery of Aadhaar cards to residents was equally broken.[333]

Due to the decentralised nature of the enrollment process, private contractors were appointed by enrollment agencies and were not verified by the UIDAI. Mismanagement of records and data transfers compromised the security and integrity of the data at enrollment centres resulting in breaches. [334] The UIDAI responded by restricting the issuance of Aadhaar cards to post-offices and designated banks. The village-level private operators rendered idle by the UIDAI's decision shifted to providing illegal access to UIDAI data and "Aadhaar services" like printing Aadhaar cards. This has spawned an industry of data brokers anonymously selling unrestricted access to any Aadhaar number over WhatsApp for Rs 500.[335] It opened up multiple avenues for creation of fake IDs, and illegal and unethical trading of identities. For example, a software patch available for 35 USD lets anyone, anywhere in the world generate an Aadhaar number.[336]

Reports suggest the CIDR has been breached multiple times, potentially compromising the records of all 1.3 billion registered citizens.[337] Security researchers have reported hardware and software vulnerabilities in the Aadhaar app for the Android ecosystem which could be used to access the information of Aadhaar users.[338] Security vulnerabilities associated with Aadhaar have increased as its use has expanded.[339] Lax cybersecurity protocols and measures have resulted in large-scale data breaches, exposing the records of citizens.[340]Recently, law enforcement busted an inter-state cyber criminal gang using cloned thumb impressions to bypass fingerprint authentication and commit financial fraud using the Aadhaar enabled payment system.[341]

These breaches and incidents raise questions about the reliability of Aadhaar for establishing a unique identity and expanding its use in the digital economy. It continues to deny any and all security breaches, dismissing concerns raised by researchers and activists as conspiracy and propaganda.[342] It ignored these early failures because addressing them would lead to deactivation of Aadhaar numbers and slow down enrollment.[343]Some of these issues predate the formation of India Stack, but the state, the UIDAI and the promoters of India Stack were aware of these limitations and continue to push Aadhaar as digital public infrastructure for identity authentication.

Enabling New Concentration of Power

Aadhaar enables the state to extend control over the digital identity market and accumulate data of public and private companies

using Aadhaar for their services and products. The new concentration of power is rationalised under the banner of serving consumer and business interests. Since the number was linked to biometrics it was a permanent form of identity, and loss or movement would not require re-enrolment or impact accessibility for citizens. By linking biometrics with Aadhaar the state reframed biometric data as an asset that can be traded by citizens to access services and entitlements, enabling them to derive value from their data.

The introduction of a government-issued digital identity was justified to improve welfare and other service delivery. By simplifying the KYC process, taking it online and linking authentication with biometrics, Aadhaar was supposed to lower transaction costs for public and private institutions and help improve service delivery. End users and improvements in service delivery were critical not only to justify the creation of a biometric authentication market but also a key part of the public narrative and political advocacy to create and secure legislative and legal support for Aadhaar.

To some extent, Aadhaar has succeeded in eliminating inefficient practices in welfare delivery. For example, ration cards were issued at state level and therefore, it was difficult for migrant workers to use it in their state of work. Schemes like “One nation, one ration card” which linked state issued ration cards to Aadhaar, definitely helped in making the system more efficient.[344] The problem comes from Aadhaar’s function creep. Failure to define the scope and boundaries of Aadhaar's application has led to it being embedded as a de-facto universal ID and an authentication tool.

Under the Aadhaar Act, the UIDAI has been granted ownership of the biometric data stored in the CIDR as well as the data collected under the Citizenship Act. Linkage of Aadhaar to public and private services has expanded the data collected by UIDAI to include mobile numbers, e-mail addresses, bank accounts, personal and government documents as well as information about services being accessed by citizens.

Enabling Accumulation & Use of Identity Data

During the Aadhaar hearings, the government and the UIDAI argued for upholding clause 57 of Aadhaar Act which allowed Aadhaar to be used by private entities, on the grounds that it was an enabling provision which expanded the choice for Aadhaar holders. The Supreme Court's decision to restrict private entities from using Aadhaar clipped the wings and jeopardised the investments of the private sector, which had built business models around Aadhaar-based authentication. Despite the ruling, the Union government and the UIDAI have managed to restore private sector access through tweaks in various rules and regulations.

In October 2018 a carveout was created for private sector firms involved in welfare delivery like banks and financial institutions to continue using Aadhaar-authentication or eKYC services or operate Aadhaar-enabled payment systems. These firms were allowed to provide services not related to subsidies using "digitally signed electronic form of Aadhaar which allows identity to be verified online without pinging the UIDAI server."[345] To avoid contempt of court charges, the UIDAI forced private firms to provide an undertaking that they will use biometric authentication only for the delivery of subsidies and take full responsibility for non-compliance.[346]

In March 2019 the Union government promulgated the Aadhaar and Other Laws (Amendment) Ordinance which allowed private sector businesses to apply for eKYC access with the Finance Ministry. Access is granted if the regulator is satisfied that the purpose for using Aadhaar authentication is "necessary and expedient" and after the UIDAI has determined the company meets compliance standards.

The Aadhaar and Other Laws (Amendment) Act passed in July 2019, repealed the Aadhaar Ordinance, and amended several provisions of the 2016 Aadhaar Act, the Indian Telegraph Act (ITA), 1885 and the Prevention of Money Laundering Act. As part of the changes ushered in by the Supreme Court judgement, the Union government clarified that Aadhaar may be made mandatory for the provision of any service only by an act of Parliament and no person shall be denied any service for not having an Aadhaar number. The Act provides for the voluntary use of either online or offline Aadhaar-based authentication.

Under the new law, a private entity may be allowed to perform authentication through Aadhaar, if "permitted by law", or is "specified by the central government in the interest of the State" and if the UIDAI is satisfied that the entity is compliant with "certain standards of privacy and security." The amendments also modify the regime that allows the state to access data from the UIDAI. Restrictions on security and confidentiality of Aadhaar-related information are waived off for complying with order from the High Court or Supreme Court or in the interest of national security. Advancing the rights of the citizen, the new law allows the individual to register complaints in certain cases, including impersonation or disclosure of their identity.

The amendment requires fees, grants, and charges received by the UIDAI to be credited to and used for expenses of the UIDAI, including salaries and allowances of its employees. The government has established a separate fund - the Unique Identification Authority of India Fund for the purpose. The UIDAI's powers have also been expanded. It can issue directions to enrolling agencies, requesting agencies, and offline verification-seeking entities for the discharge of its functions and may initiate a complaint against an entity for failure to comply with the Act its directions, and/or failure to furnish information required by the UIDAI.

The Aadhaar Authentication for Good Governance (Social Welfare, Innovation, Knowledge) Rules were passed in 2020 [347] to allow use of Aadhaar authentication on a "voluntary basis" by government ministries or departments or state governments. The voluntary use of Aadhaar authentication is allowed for broad and vague purposes like "in the interest of good governance", "preventing leakage of public funds", "dissipation of social welfare benefits", "promoting ease of living of residents" and "enablement of innovation and the spread of knowledge."

The MEITy has proposed amending the Good Governance Rules to include a framework for allowing non-government entities to undertake Aadhaar authentication for "promoting ease of living of residents and enabling better access to services for them" in addition to the purposes listed above. "Any entity" seeking to use Aadhaar authentication for permitted use-cases is required to submit a proposal to the central/state government explaining why it is "in the interest of the State." The proposed amendment is in contravention of the SC's judgement, and expands the power of the state to compel private entities to use Aadhaar.

As per the government, 1.3 billion Aadhaar numbers have been issued, nearly 650 state government and 315 Central government schemes leverage the Aadhaar ecosystem and biometric authentication for identification and authentication of beneficiaries, transfer of benefits, and ensuring de-duplication. Given the scale of adoption and use the UIDAI has amended the Enrolment and Update Regulations to require Aadhaar number holders to "update their supporting documents in Aadhaar, at least once" after each 10 year period. [348] The move enables the UIDAI verify Aadhaar numbers and rectify or update demographic information. It is not as yet clear whether the UIDAI is considering mandating biometric updates.

Data Sovereignty and Digital Payments (Cashless Layer)

Despite being a cash-dependent economy, India has managed to reduce the share of currency in circulation (CIC) in payments from 88 percent in 2016 to 20 percent in 2022.[349] India is the third largest digital payments market in the world, after the US and China. This has been achieved through the state exerting control over the digital payments market while simultaneously opening it up for new players. By framing digital payments systems as digital public infrastructure, the government is attempting to export it to other countries.

Restricting Access to Digital Payments Market

Recognizing the critical role of payment systems in facilitating economic activity, and in the pursuit of sovereignty the state extends control over the payments market in different ways. It enacted the PSS Act to create a legal basis for payments in India. The law does not define the role or lay down statutory mandates for payment systems providers and operators. It does designate RBI as the apex authority and grants it powers to frame regulations. As a result, the regulatory framework for payment systems including issues like interoperability, risk management, or consumer protection has been developed through subordinate legislation, circulars or guidelines.[350]

The absence of clear obligations for both payment service providers and the regulator under the PSS Act, has created uncertainty for businesses. It has led to the RBI, which is also an operator of payments systems like RTGS and NEFT, being given the powers to exercise regulatory control over the functioning of India's payments market. For e.g. the PSS Act does not specify whether banks are required to obtain RBI's authorisation to operate payments systems in India. The RBI has issued guidelines requiring banks to obtain RBI's approval and non-banks to seek RBI authorisation for operating payment systems.[351] Similarly, banks can issue prepaid payments instruments if they meet eligibility criteria set out by the RBI and after obtaining its approval.[352] In the absence of checks and balances for the regulator the current arrangement carries governance risks and may impact innovation.

The roots of the NPCI lie in economic competition between banks and card payment network operators. It was established to enable public-private banks to come together for the development of retail payments. Today, the NPCI owns and operates several payment systems including the RuPay, IMPS, AePS, APBS, BBPS, NACH and the National Electronic Toll Collection (NETC). NPCI also operates NFS and the Cheque Truncation System (CTS) on behalf of RBI.

The NPCI was not created by the parliament, or by a central/state government but through RBI's authorization. Initially, promoted by ten major banks, the shareholding has since been diversified to 66 banks. While the shareholding is diversified and hence there is no single promoter, capital support is provided from member banks, a majority of which are public sector banks. The state retains ownership through the public sector banks which hold the majority stake and make up most of NPCI's board. The RBI also nominates a director to the board and approves the appointment of NPCI's Chairman and Chief Executive Officer (CEO). In 2008 the RBI appointed AS Hota who had served as RBI's chief general manager as CEO. Following his retirement in 2017, the RBI overruled the NPCI board to appoint another CEO of its choice. The decision prompted board directors to file notes of dissent calling out the central bank’s actions as an attack on “good governance.”

NPCI is owned, controlled, substantially financed directly or indirectly by the government. The NPCI and NPCI International Payments Limited (NIPL), its wholly owned subsidiary created for the deployment of RuPay and UPI outside of India,[353] are audited by the public auditor.[354] Due to its incorporation as a Section 25 company, the NPCI is not regulated as a public entity and does not fall under public accountability mechanisms like the Right to Information (RTI) Act.

The Wattal Committee had recommended separating NPCI's role as owner of the payment system from its role of a participant in the payment market. It had recommended diffusing shareholding and the diversification of the NPCI board of directors with the appointment of public interest and non-bank directors. While the RBI has supported diffusion of shareholding it is not keen on NPCI being listed as profits may create "perverse incentives."[355]

As the operator and infrastructure provider of payment systems in India the NPCI has economic interests in restricting access / limiting competition in the payment market. NPCI used its regulatory capacity to give banks a monopoly over the creation of the UPI Id. Similarly, the UPI interoperability feature was initially designed to benefit the payment system operator.[356] NPCI allowed the adoption of UPI by non-member banks but kept wallets out. Updates to the interoperability rules were stalled preventing wallets from tapping into the network effects from the pre-existing customer base.[357]

In 2017, Walmart-owned PhonePe which partnered with YesBank to provide digital payments services was allegedly found to be engaging in restrictive practices. Instead of asking the NPCI to intervene, ICICI which is a NPCI-member bank blocked PhonePe's VPAs citing “security related concerns about the access to UPI data to a non-banking application” and "violation of UPI guidelines of interoperability and choice".[358] ICICI bank took unilateral action against another bank's application without transparency or consulting with the NPCI or RBI. The move impacted PhonePe users but more importantly raises questions about both the NPCI and RBI's[359] neutrality and governance capabilities.

Restricting Access to Digital Payments Data

In April 2018, the RBI directed all banks and authorised payment system providers to store payments systems data related to user transactions 'collected, processed, carried in India' including ‘full end-to-end transaction details’ and ‘payment instructions’ only within India’s national boundaries. The RBI gave payment providers six months to comply with regulations and required to submit system audit reports to confirm compliance. Under the restriction based strategy, India’s central bank has framed the need for localisation in a well-known but still utterly false premise: ‘security of data is dependent on the location of data’.[360] The RBI reasoned that data localisation is necessary to retain regulatory oversight or ‘control of data' as data stored outside the sovereign boundaries of the country curtails its ability to “monitor payments activity”, ensure information security and guarantee citizens’ rights over their data.[361] India’s law enforcement agencies (LEAs) supported data localisation on the grounds that "colonisation of Indian data has to end due to national security concerns that are getting sharpened amid the government’s growing push for Digital India."[362]

The RBI rationalising data localisation for investigations overlooked mechanisms such as mutual legal assistance treaties (MLATs) that enable states to cooperate to obtain access to data. Arguably, negotiating or setting protocols for gaining access to data is easier when data centre operators, network and service providers are physically located under the jurisdiction of LEAs. However, even before the data localisation mandate domestic payment networks like UPI and foreign card networks or banks like Visa, Mastercard and American Express were storing a superset of all transaction data processed by them in India. The RBI had access to and was monitoring this data.

Restricting data within the jurisdiction of a country, does not entitle LEAs to have meaningful access to data as ultimately, the entity in custody or possession of data has control over data. As owner and operator of IMPS and UPI, the NPCI controls the digital payments market. The UPI Id and the VPA are linked to every transaction over the network, transforming UPI into a centralised server. NPCI has access to user credentials associated with the UPI Id and VPA as well as the data stored in the UPI Common Library embedded in each PSP app.

Centralising data in local servers, whether operated by domestic or foreign companies, makes data more vulnerable to domestic and foreign security threats. Data localisation does not guarantee accountability towards data stored within the territorial borders of India. In India, unauthorised sharing of payments data is on the rise and surveillance capacities of the government have grown unchecked and activities are carried out with little oversight adversely impacting the rights of citizens.

Although the RBI justifies restricting access to data in the interest of establishing and protecting rights of citizens over their data, RBI's ongoing efforts for linking payments data to Aadhaar and expanding use of payments data contradicts this view. In fact, localisation of payments data helps the RBI to carve out and retain control over a subset of personal data which may lead to contestation with the data protection authority proposed under the draft data protection law. The data protection legislation in India has been stuck in the drafting stage since 2018.

Uncertainty about technical or institutional arrangements around data localisation mandate and concerns about costs to build the digital infrastructure required to store data locally created pushback from most of the payment providers. Several banks and PSPs lobbied with the Ministry of Finance and the RBI for relaxation.[363]Banks argued that they should be kept out of the scope of the directive as they were licensed entities and the RBI's regulations provided for separate data confidentiality requirements.[364] In June 2019, the RBI released frequently asked questions reiterating the mandate's applicability for both banks and PSPs.[365]

Despite having wide regulatory powers, the RBI needed support for ensuring compliance and roped in the NPCI to enforce data localisation through contracts with entities on its network. The NPCI directed payment service providers, banks, and other participants that operate through its UPI infrastructure to comply with the mandate. By outsourcing enforcement to NPCI, the RBI expanded the localization mandate to unlicensed entities like non-bank PSPs and extended NPCI's control over payments data generated in India. Arbitrary enforcement has disincentivized and created a risky environment for foreign firms.

Court documents reveal that

data localisation mandate used to stall the commercial launch of WhatsApp Pay in India.[366]

WhatsApp had sought permission to launch UPI payments for all users and the RBI and NPCI began monitoring WhatsApp's compliance with data localisation in April 2018. WhatsApp was ready to go-live with its UPI service WhatsApp Pay in November 2019 but the RBI intervened to delay roll-out. The RBI asked the NPCI to ensure five specific data fields were not being stored by WhatsApp and that the data being stored by the company abroad did not contain payments data.[367]

The NPCI granted WhatsApp approval in November 2020 to go live on UPI in the multi-bank model but was authorized to roll-out in a graded manner.[368] Initially a cap of 20 million users was placed which was increased to 40 million in November 2021. In April 2022, NPCI allowed WhatsApp to extend the user base for its payments service to 100 million.[369] The new limit does not cover WhatsApp's 500 million user base in India but will allow it to compete with Google Pay and PhonePe. The basis for NPCI treating WhatsApp differently from other platforms and the rationale for the limited users mandate by NPCI to WhatsApp has not been laid down and is being challenged in courts.[370]

Two years after the RBI's mandate the NPCI in May 2020 sought a system audit report from all payment providers on its UPI network. Payment providers were asked to clearly indicate which components of its transaction data flows and application architecture are located geographically.[371] The report also asked providers that defined payment data is stored only in India and no copy or backup is maintained outside the Indian jurisdiction in any form.

In April 2021, RBI moved on from negotiating applicability with payment providers or following up on compliance and started sanctioning payment providers for their failure to meet data localisation norms. Mastercard, American Express and Diners Club were barred from acquiring new customers for an indefinite duration. The sanction is likely to have a significant impact on these firms and indicates that entities availing services from banks and PSOs under contracts could be expected to similarly comply through penalties.

Under the data sovereignty approach India is pushing through with data localization through state-market cooperation, but in the absence of clear and defined terms and through opaque and arbitrary enforcement. The effects of such state and market cooperation to restrict payments data are yet to play out; but the [372] benefit for Indian companies is already visible, with corporations like the Adani Group, Bharti Airtel and Reliance Jio investing in data centers in India.[373] Given the importance of UPI, greater transparency is needed around RBI and NPCI's decision-making and policy enforcement of data localisation.

Enabling New Concentration of Power

The number of RuPay debit cards in circulation has surpassed one billion. UPI crossed the 1 billion transaction threshold in October 2019, three years after its introduction. According to NPCI data, UPI emerged as the preferred mode of payments for small denomination P2P transactions among users across all income groups and approximately 74 billion transactions worth INR 125.94 trillion were conducted using UPI in 2022.[374]

The use of UPI and RuPay outside of major cities, and its integration for accessing government services or utilities and in commercial transactions across sectors like retail, health and telecom has contributed to widespread adoption.[375] The introduction of features like UPI AutoPay feature that simplify recurring transactions, and interoperability between RuPay and UPI enhances the convenience and accessibility offered by these payment modes. RuPay cards can be easily linked to UPI Ids, enabling users to conveniently make payments over UPI platform through their RuPay cards. Similarly, UPI can be used to make payments on the RuPay network, withdraw cash from ATMs and make purchases at merchants that accept RuPay cards.

The underlying tech for RuPay and UPI is owned and operated by the NPCI, but their widespread adoption has been achieved with the state's backing and by partnering with the private sector. The NPCI brought in iSpirt volunteers and fintech startups like Juspay to develop the UPI and the BHIM app.[376] These handful of individuals and private firms developed the infrastructure and standards for UPI. Over the years the UPI network has expanded to include 382 participating banks, and over 50 million merchants.[377] Despite the growth in the number of transactions, the user base is still small in proportion to the total economy. UPI contributes only about 3.3 per cent to the digital payments market.[378] NEFT and RTGS continue to dominate the market for high-value transactions.

Due to the government's mandate, business entities with an annual turnover in excess of 500 million cannot refuse to accept payments through UPI and RuPay debit cards. The government has also introduced a zero-MDR regime, under which consumers and merchants do not have to pay fees to acquirer banks or non-bank service providers for transactions on RuPay and UPI. In contrast, all non-RuPay card transactions are chargeable by banks and tend to hurt merchants' margins.

The subsidy applies equally to large and small businesses with an annual turnover in excess of 500 million. The intervention has led to merchants, small retailers, stores and vendors across the country taking to digital payments in a big way.[379] The UPI system currently processes more P2M UPI transactions than P2P UPI transactions.[380] The volume of P2M transactions is driven by low value transactions below INR 500 as UPI has reduced the cost of transaction to almost zero. However, 70 percent of the transaction value for P2M UPI payments came from processing transactions over INR 2000 to large merchants and ecommerce retailers.

Enabling digital payments requires investments in payments acceptance infrastructure and settlement guarantee or fraud risk management funds, user-friendly apps, and merchant distribution networks. Banks and PSPs bear the costs of undertaking KYC, popularizing payment modes through rewards or cashbacks, software and customer service development. Zero MDR regime has curtailed the revenue from transaction charges which was being utilized towards these costs and investments. Adoption of digital payments allows banks to save on costs of currency management however the costs of processing large volume small denomination UPI transactions without profit is not a priority for banks which have other sources of income. The withdrawal of MDR has removed the financial incentives for banks and PSPs to promote UPI and RuPay, allegedly the objective of this policy move. The absence of revenue has pushed banks and PSPs to rely on the financial support of the government instead of pursuing innovation in digital payments.

Banks have a very small market share in UPI and PayTM bank occupies more than an 80 percent share in the segment.[381] Currently, two non-bank apps funded by global conglomerates Google Pay and Walmart-owned PhonePe constitute around 81 percent of the market. Fintech companies have succeeded in the UPI ecosystem as they have the resources to sustain the zero MDR scheme and fund cashbacks. Incumbents like Google Pay have gamified cash-backs to a luck-based lottery system to retain their dominant position.[382] This is forcing new players like WhatsApp Pay to resort to the same tactic and preventing smaller players from entering the digital payments market.[383] Cashbacks have proven to be successful but are not sustainable, and scaling them back slows down adoption and use of UPI.[384] After MEITY stopped giving out cashbacks, BHIM's transactions on UPI declined.[385]

The RBI was initially not in favor of the policy as subsidizing digital payments through zero-MDR is not a viable solution for the long term. Banks are opposing the withdrawal of MDR charges on UPI and have claimed this will lead to the collapse of the payments industry.[386] Zero-MDR has also impacted market share of RuPay debit cards which has remained stuck at the same level for the past three years.[387] The Indian Banks' Association has approached the government seeking a restoration of MDR on the usage of RuPay debit cards on the grounds that MDR is essential, to foster sustainability, enhance payment network security and enable continued investments in cutting-edge technologies and innovative payment solutions.[388]

The Finance Ministry continues to rationalise the use of public funds for subsidising zero-MDR as investments in the cashless economy. Financial support for zero-MDR was INR 654 crore in 2018,[389] INR 1010 crore in 2019,[390] INR 188.9 crore in 2020[391] and INR 1500 crore in 2021. Financial support of USD 318.4 million has been announced for 2022-23.[392] The fiscal support is expected to increase further but is a fraction of INR 8000 crore costs estimated by the industry.[393] Banks are also allegedly appropriating the compensation and the government's financial support is not reaching payment aggregators like PayU.[394]

Recently, the RBI's discussion paper on payments charges sparked speculation the zero MDR policy would be rolled-back.[395] However, the finance ministry has clarified[396] that

no charges would be levied on UPI as it is a "digital public good"

and "concerns of the service providers for cost recovery have to be met through other means." Recognising that just because UPI is a public good, private entities cannot be expected to provide it for free, the RBI has decided to impose interchange fees on UPI transactions made through PPIs such as wallets. As of April 2023, merchants processing UPI payments above INR 2000 through wallets will have to pay an interchange fee of up to 1.1 percent as wallet-loading service charges.[397] Currently the interchange fees are in the range of 0.5 to 1.1 percent on different services and the NPCI will review by 30 September 2023.

UPI opened up the banking for new players but has led to concentration of UPI volumes in the hands of a few players. Proponents of data sovereignty rationalize the market concentration by claiming, "100% of UPI traffic flows through the Indian banking system."[398] But this narrative does not address the challenges of sustaining growth or issues arising from market concentration.

The NPCI has responded to these challenges by imposing a 30 percent transaction volume cap on dominant players on UPI. However the deadline to meet the market cap has been deferred to December 2024 citing UPI's current usage and future potential.[399]The NPCI has also put market share caps for new players as demonstrated through WhatsApp Pay's roll-out with a limited number of users. NPCI's approach of capping the market share does not restrict incumbents from continuing to offer cashbacks to retain their position or the risk of market caps leading to the formation of oligopolies.

Recognizing the limitations in NPCI's governance capabilities, and to mitigate risks arising from it being a single point of failure, the RBI explored introducing an alternative to the NPCI called New Umbrella Entity, or NUE.[400] Unlike UPI's generic payment network, NUEs would build interoperable customized networks based on use-cases, their business model or distribution capabilities.[401] The NUE framework required a minimum paid-up capital of INR 500 crore and no single promoter or promoter group could have more than 40 percent investment in the capital of the NUE. Shareholding would be diluted to a minimum of 25 percent after 5 years of the commencement of business of the NUE. Several players in the Indian banking and payments landscape expressed interest and submitted bids for licenses to operate NUE. [402] The RBI has abandoned plans for the NUE due to failure of consortiums to propose "any innovative or infrastructural solutions",[403] and "data storage and localization issues." [404]

The development of digital payments has been led through state-market cooperation and has concentrated power in the hands of a ‘not-for-profit’ company controlled by a number of promoter banks. In pursuit of data sovereignty, the state is facilitating the growth of NPCI and its digital payment products and services through policy and public spending. The concentration in the market and gaps in the governance capabilities of the RBI and the NPCI calls for creating an independent payments regulator in India.

Enabling Accumulation & Use of Payments Data

With the government's assurance that UPI will continue to remain free, the reduction in cost of transactions and zero MDR digital payments players can no longer be dependent on earning revenue from facilitating the transfer of funds. As banks and payment providers seek new avenues of growth data linked to a transaction has become a valuable resource. The integration of UPI in the digital economy has resulted in an explosion of different types of data such as transaction data (number, value, time, date), user data (bank account information or transaction history), device data (device, operating system, PSP or software), location data, merchants data (business details, transaction history, or sales) and data on the performance of the UPI platform.

Over the years, NPCI has brought about regular updates to UPI that appear to be driven by a goal of pushing the data economy and have opened doors to the entry of new players. Under the accumulation strategy the expansion of the scale and scope of UPI is being promoted under the banner of greater financial inclusion and financial empowerment and more recently digital public infrastructure.[405] NPCI is planning to roll out UPI payments on feature phones.[406] UPI's linkage with Aadhaar enables linkage of government issued identifiers and financial transactions, opening gateways for data collection on the financial behavior of the users and government schemes.

The UPI 2.0 introduced in August 2018 allows users to link an overdraft (OD) account and share digital invoices accompanied with collection requests, features which are aimed at transforming UPI as the rail for credit access.[407]

The NPCI has launched the UPI Lite, a compressed version of UPI designed as an 'on-device wallet' to handle high-volume, low-value merchant transactions that range from Re. 1 to Rs. 200.[408] Transactions made through UPI Lite are deducted from the wallet and not from the linked bank account, simplifying bank and transaction data for credit access. In addition to the existing facility of linkage of UPI with deposit accounts, the NPCI has linked RuPay Credit Card to UPI. The facility has expanded the scope of digital payments enabling retailers and merchants to utilizing QR codes for accepting payments through credit cards. The RBI has also expanded the scope of UPI by permitting customers to operate pre-sanctioned credit lines at banks through the UPI.[409] The move enables the NPCI to push new credit products over the homegrown payments platform, and is expected to strengthen digital lending and Buy Now Pay Later (BNPL) businesses. India Stack architects advocate for using UPI data to expand the lending market.[410]

As banks and PSPs shift their business model to aggregating and monetizing financial data of their users for use cases such as advertising and credit lending these data points have become immensely valuable.The collection and analysis of this data can provide actionable insights into the behavior and preferences of users, as well as the trends and patterns in digital payments in India. Data behemoths like Google and Walmart-Flipkart fund cashbacks and bear the costs of zero-MDR for UPI transactions in India to acquire more data points of consumers and spending patterns in India. In 2018, Paytm alleged that Google Pay was sharing data with its group companies and third parties, and for advertising purposes.

The dominance of fintechs has not translated to a significant data advantage since banks and the NPCI have access to the same transaction data as fintechs. As a consequence, UPI's architecture has evolved on the principle of 'data maximization' or collecting and sharing as much data as possible. As multiple privacy advocates have pointed out UPI 2.0 specification enables collection of vast amounts of data and all the parties involved in the UPI transaction to get a slice of the consumer's transaction data.[411] Since the data-sharing policies of UPI have not been made public it is unclear what these data access and sharing arrangements are.

Allowing large-scale mining and analysis of the income and spending patterns of consumers enabled by UPI needs to be assessed against the fact that access to financial data poses privacy risks and India does not have a data protection law. In an ecosystem where privacy rights of individuals are gaining greater currency, it is crucial that regulatory changes do not nudge industry players into undermining these rights.

As part of data sovereignty strategy the RBI has been working on expanding acceptance and use of UPI in other countries.[412] As one of the largest remittance recipients in the world India has prioritised creating acceptance of UPI in countries from which it receives the largest remittances. India has partnered with Australia, France, Hong Kong, Singapore, Saudi Arabia, Oman, U.S., the U.K., and the United Arab Emirates to enable cross-border payments using UPI.[413] India's neighbours and Nepal have also started using UPI for cross-border payments. The ambitions of creating global acceptance of UPI is also fueled by India's desire to mitigate geopolitical risk. In February 2022, the U.S. and its Western allies blocked Russian banks' access to the international payments system Society for Worldwide Interbank Financial Telecommunications (SWIFT).[414] The decision was part of the economic sanctions against Russia's invasion of Ukraine and has crippled banks and financial institutions in Russia.[415] The move raised concerns in India which has been subjected to economic sanctions by the west in the past and continues to export resources from Russia.

India's anxieties about building alternatives to U.S. and E.U.-led payments networks resonates with other developing countries, and China which has been developing its own alternative to SWIFT, the Cross-Border Interbank Payment System (CIPS).[416] The ban has provided an opening for India to forge partnerships with countries to expand the use of UPI towards establishing it as an alternative to existing global payment networks like SWIFT.[417] Indian entrepreneurs and investors involved in the development of the cashless ecosystem in India support exporting UPI as a way to launch Indian startups into the global market.

Securing Digital Payments Infrastructure

According to the Chairman of the Parliamentary Panel on Finance,. As noted by the Chairman of the Parliamentary Panel on Finance, the increase in digital transactions through platforms like UPI has also brought about a rise in cybercrimes and vulnerabilities.[418] However, there is a lack of accessible data regarding payment frauds on the systems managed by NPCI. The Finance Ministry revealed that in 2022-23, there were over 95,000 fraud cases related to UPI transactions, compared to 77,000 cases in 2020-21 [419] and 84,000 cases in 2021-22. These numbers are likely to be much higher since many affected users do not report fraud, and payment apps are not obligated to report UPI-related frauds to NPCI or the RBI.

Financial frauds and scams have become an industry, [420] with hackers and cybercriminals constantly adapting their tactics to exploit vulnerabilities in these systems and gain unauthorized access to user information and devices. These criminals employ various methods, such as using multiple SIM cards, fake identities, fraudulent websites or payment requests, unauthorized QR codes or payment links, bulk messages or targeted ads. They may even acquire access to existing bank accounts using fake KYC documents, including those opened under the PMJDY financial inclusion scheme. Scams targeting UPI users exploit local consumer experiences, behaviors, and the lack of digital literacy. A recent study highlighted that social engineering techniques, which are cost-effective and highly successful, are widely employed to deceive consumers and steal money from their accounts.[421] For instance, fraudsters use incentives like cashbacks and free deliveries to trick consumers into revealing their UPI ID or sharing sensitive details like one-time passwords. As consumers willingly disclose information that enables fraudulent transactions, banks are often reluctant to address these frauds. The use of malware in PoS machines and ATMs is also increasing, and such deceptive methods are not limited to UPI or RuPay but are industry wide-challenges that have become more sophisticated and difficult to detect.

The RBI Working Group has recognized that certain payment systems are of systemic importance, as their failure could disrupt the entire financial system. The group recommended periodic review of the classification of Systemically Important Payment Systems (SIPS). In line with this, the RBI designated the RTGS system, owned, operated, and regulated by the RBI, as a SIPS due to its significance in handling high-value transactions. Despite the significant growth and promotion of UPI transactions as digital public infrastructure, the IMPS, which processes UPI transactions, has not been designated as a SIPS. It is important to note that the existing regulatory framework under the PSS Act does not differentiate between SIPS and non-SIPS.

The NPCI provides and manages infrastructure underpinning some of India's most crucial payment systems including the IMPS, UPI, NFS. The Watal committee emphasized the need to classify NPCI as a Critical Payment Infrastructure Company (CPIC) and subject it to open access obligations due to its crucial role in security. However, NPCI enjoys considerable flexibility in complying with data security standards and policies. In 2019, the National Cyber Coordination Centre (NCCC) conducted an audit of NPCI to evaluate its defenses against cyberattacks. The audit identified several "critical" and "high" risk security vulnerabilities, such as unencrypted card numbers in the NPCI database and server logs containing unencrypted RuPay card numbers.[422] Vulnerabilities stemming from memory safety issues allowed hackers to exploit coding errors. Furthermore, NPCI's operating systems and mail servers were not up-to-date and lacked sufficient malware protection. The NCCC stressed the importance of proper governance at NPCI based on these findings. In response, NPCI defended itself by claiming compliance with data security standards set by the PCI Security Standards Council. It stated that regular audits were conducted in the interest of security, and senior management reviewed and remedied any findings to the auditors' satisfaction.

Recognizing the need for supervision, the RBI updated the oversight framework for payment entities in 2020.[423] Under the new framework, NPCI was designated as a System Wide Important Payment System (SWIPS) due to the substantial volume of transactions processed in its payment systems. NPCI was also required to assess itself against the Principles for Financial Market Infrastructures (FMI).[424] The term FMI generally refers to systemically important payment and settlement systems used for clearing, settling, or recording financial transactions.

The PFMI guidelines are a set of international standards applicable to payment systems under the PSS Act. NPCI has published a disclosure report on its compliance with the PFMI guidelines in 2022, in accordance with regulatory requirements.[425]

According to the NPCI website they have implemented a strong cybersecurity strategy that complies with international standards for information security and business continuity management. Reputed firms conduct regular security assessments and audits to ensure the effectiveness of these measures. However, security researchers have highlighted [426] that many security audits in organizations like NPCI are performed by vendors chosen based on low cost rather than expertise. The absence of independent auditors makes it challenging to verify NPCI's security claims and understand if it is addressing security concerns adequately.

Whistleblowers have played a crucial role in exposing security practices of tech companies and enabling regulators to enforce existing policies. In a 2017 audit by the RBI, NPCI was found to have improper whistleblower policies, lapses in internal auditing processes, and a lack of risk awareness and culture. A subsequent audit in 2019, mostly redacted by the RBI citing the need to protect India's and the NPCI's economic interests, further emphasized the need for accountability and stronger enforcement mechanisms.[427] UPI has been misused for fraud on a significant scale, leading payment companies to invest in setting up risk mitigation departments. PSPs rely on algorithms and third-party services to review and scrutinize suspicious accounts and transactions. To combat fraud proactively, companies like PhonePe have developed scoring systems based on the transaction history of merchants.[428]

Not only is it challenging to keep up with criminals who can easily switch to other accounts or tactics, institutional mechanisms to facilitate cooperation, information sharing, and coordinated action among payment companies are missing. The existing fraud redressal framework is also limited due to the lack of incentives for various actors to pursue fraud cases. PSPs focus on increasing transaction numbers and prefer to avoid transaction or data flow disruptions. When fraud occurs, victims often approach banks that have no control over transactions made through apps and redirect consumers to LEAs. LEAs typically respond only to cases where the victim has lost a significant amount, redirecting victims of smaller frauds to local police stations ill-equipped to handle such cases. Investigating UPI frauds is also time-consuming as the bank account number linked to a UPI ID is often unknown due to tokenization, and victims may have used someone else's UPI ID for the transaction.

To address these security gaps, the RBI is considering implementing stricter security controls for payment entities operating in India. In June 2023, the RBI released draft directions for non-bank PSOs and their contracted entities. These proposed directions include establishing a Security Operations Centre (SOC) for proactive monitoring of network logs, managing security incidents, and reporting any unusual incidents to the RBI within six hours of detection. PSOs must adopt a secure-by-design approach for developing new services or products and conduct risk assessments before making changes to existing infrastructure, products, or services. Safeguards against phishing and risks posed by vendors and API access must also be in place. Access controls should be implemented by assigning digital identities to individuals with IT environment access to enable fraud monitoring and detection. The regulations propose the appointment of dedicated nodal officers to liaise with customers and LEAs regarding fraudulent transactions. The Indian government has also made it easier for victims to report cyber frauds, including UPI-related ones, through improvements to the National Cybercrime Reporting Portal (NCRP).[429]

Data Sovereignty and Data Sharing (Consent Layer)

The Consent layer is still in the early stages of development with evolving guidelines and industry practices. The consent layer is being implemented in the financial sector through RBI's Account Aggregator's framework. Currently there are nine AAs with an operating licence and another eight have approval in-principle from RBI. Building on the principle of reciprocity, implementation for FIPs and FIUs has been categorised into five stages, viz., *live*, where it is available for end users; *live-enabled* where it is in the final stages of production; *testing,* where the service is being tested with at-least one AA; *in-development* where the service is still being developed; and *under-evaluation* where the institution has not yet begun developing the service.

The AA system is yet to become mandatory for any of the ecosystem partners which includes banks, credit companies, and investment advisors. The state restricts access to the ecosystem by requiring FIUs or FIPs to be regulated by at least one of the financial system regulators – RBI, SEBI, IRDA and PFRDA. The commercial arrangements between FIUs and AAs are left to the market. From the latest data available, 4.02 million bank accounts have been linked to AAs and the cumulative count of consent requests successfully fulfilled is 3.9 million.[430] The data required to fully understand the level of market and data access and impact on competition is not available.

Under the accumulation strategy, the adoption of AA framework is being pushed to improve access to financial services. According to industry estimates, 50 percent of the lending disbursed through AAs were to MSMEs and 20 percent of the unsecured loans given by digital platforms were channelled through AAs.[431] The regulator RBI and self-regulatory body Sahamati are working on a proof of concept to extend the AA framework to people without smartphones or people with low digital or financial literacy.

There are indications that the AA framework, which is presently limited to enabling sharing of financial data, may be expanded to integrate other types of information. In August 2020, RS Sharma, Chairman TRAI and a senior bureaucrat who had worked alongside Nilekani on the implementation of Aadhaar, made the case for telecom service providers to be included as FIUs under the AA framework as telecom data like mobile recharges often constitutes the first digital footprint of a low-income household. A steady history of telecom service could help formulate a basis for credit history. In November 2022, the RBI brought the goods and services tax network (GSTN) under the ambit of the AA framework as a FIP, allegedly to facilitate lending to micro, small and medium enterprises (MSMEs).[432]

Architects of India Stack believe that enabling an electronic consent artefact to retrieve, collect, consolidate and organise data from people, will grant them control over their data. Electronic consent artefacts enable users to access their data residing across various repositories and share this info, in a highly granular fashion and for a predefined time, with service providers. The consent layer of India Stack is conceived and designed to make the collection and flows of data visible to the individual. The approach aligns with both the restriction and accumulation strategy of data sovereignty.

Techno-legal frameworks like DEPA are framed as enabling users to exert ownership and exercise choice in deciding which data can be shared, with whom, and for what duration. If DEPA is adopted at scale, the argument goes, it could become the default privacy framework for accessing financial information and services in India. And if DEPA takes off in the financial sector, the model of consent collection and management can be extended to other sectors such as healthcare and telecom.

DEPA establishes a specific and tailored model of data protection which frames personal data as a tradeable asset and encourages users to exercise rational choice to disclose data for economic gains. The structure of DEPA emulates existing notice and consent mechanisms that relies on self-management of privacy by users where they have to agree to the terms and conditions in order to access services. This approach of self-management views privacy in a series of isolated transactions guided by decision-making of particular individuals. The DEPA framework goes further; consent is obtained and aggregated via a uniform interface or a standardised consent artefact rather than being collected website by website.

Relying on user consent, the DEPA overlooks a broader issue: while *citizens may have preferences, often these are difficult to articulate* or *express*. By allowing users to consent to the sharing of their data the AA framework grants users control over their data. The level of granularity that is required for informed consent, however, requires digital literacy, investment in time and effort from users which is unaccounted for in the DEPA's architecture.[433] Because consumers give consent under conditions of uncertainty, there must be clear limitations on data collection and use, otherwise consent may not be respected or be meaningful in upholding rights.

Part 6. Conclusion

The emergence of India Stack is result of three important shifts in the relationship between the state and the digital economy:

- **State-market collaboration.** India Stack was kickstarted through the National Information Utility (NIU) framework. This model was operationalised initially through government outsourcing of digitisation of existing services and the development of new mechanisms for the delivery of public services to software developers.

- **Scale**. State capacity is being leveraged by private business to achieve high scale. The framing of “built at scale” allows India Stack to claim labels like *digital public infrastructure* and *digital public goods.*

- **Data sovereignty**. State support of India Stack stems not from addressing market failures but as part of its efforts to *extend sovereignty over data,* India Stack recalibrates the state's approach to governance of data, extending control sometimes by enabling accumulation and sometimes by restricting access to data, but in both cases attempting to enact a nationalistic notion of data sovereignty.

Despite the controversies and questions about its long-term stability, India Stack shows no signs of slowing down. The Indian government is working to export India Stack to other countries, pitching it as digital public infrastructure at forums like the G20.

Critical industries in India have often emerged under the shadow of the state, with the state propping up public sector and private companies as national champions. It acts as an investor, provides regulatory concessions and creates demand for products and services produced by these companies. While the state would provide funding and resources initially, national champions were expected to compete with global firms in the market in the long-term. India Stack combines these elements with new features to produce a distinct model.

Advancements in technology have forced states to expand their capacity for effective and efficient delivery of governance and services. This has resulted in a new type of state and market collaboration for the development implementation of critical industries and tech-intensive projects. The state outsources design, implementation and monitoring functions to institutions like the UIDAI and NPCI.

These institutions act as critical intermediaries helping the state design and implement projects. They manage projects on behalf of the government, bringing in independent contractors and vendors as a way of lowering costs. These institutions exercise control over the development of infrastructure and technologies through a network of outsourced contracts. Data restriction and accumulation capabilities grant them even more control over consumers, service providers, vendors enabling them to work closely with the state to achieve policy goals.

The institutions involved in India Stack enjoy the best of both worlds, using the state to expand market access and escaping regulatory oversight. Outsourcing development of large-scale technology infrastructure to institutions like UIDAI and NPCI allows the state to distance itself from failures and evade accountability for addressing challenges to improve development. India Stack represents a recalibration of the state's approach to the governance of data where it is using institutions like UIDAI and NPCI to extend control over data markets, sometimes by enabling accumulation and sometimes by restricting access to restricting access to data from important sectors.

India Stack requires investment willing to absorb losses to achieve the long-term goal of control over markets. The development trajectories of Aadhaar, UPI, Digital Locker and DEPA indicate the state's involvement and backing as an investor, along with the industry players in the banking, financial and software sectors. Describing Aadhaar, UPI, Digital Locker and DEPA as *digital public goods* enables the promoters of India Stack to seek investment from the state as well as the market.

The framing of India Stack as *digital public infrastructure* enables the state to continue to act as an investor, providing funding or subsidising costs. The state embeds India Stack products and services across various aspects of the digital economy not just with the aim of propelling innovation or addressing socio-economic challenges. Rather, as these services scale, they become sources to attract foreign investment, as is evident in the state acting as a promoter, marketing India Stack for export to other countries through various forums.

Achieving scale is another feature of India Stack, one which is critical to its ability to create and capture value from data. It aspires to serve as the foundational infrastructure for the digital economy. India Stack has emerged by linking mobiles, digital identity and payment systems to the solutions developed under its umbrella. These three elements are the building blocks of digital economy services and also what connects every citizen to India Stack. By integrating these three basic institutional units, India Stack is able to justify integrating and expanding its capabilities for the delivery of public and private services. The label of digital public infrastructure or public goods is used to pursue infrastructural ambitions.

The state is a key ally, helping India Stack amass a large consumer base. By outsourcing critical functions to iSPIRT, UIDAI, and NPCI it granted these institutions a unique opportunity to influence and shape the preferences of its 1.4 billion people. However the power of India Stack is not just anchored in the state and these institutions, it is also derived from a complex set of loosely connected private sector actors and institutions with exclusive or semi-exclusive control that are driving its adoption.

A categorization of the various India Stack components, reveals that technical specifications have been created by a closed group of volunteers. The founders claimed that the decision to operate as a volunteer-led think tank was made to maximise impact and keep costs down. However, in a video posted on YouTube, Pramod Varma, the chief architect of Aadhaar, said the reason they decided to become "volunteers" was to avoid any scrutiny under India's Right To Information Act or audits by the Comptroller and Auditor General of India (CAG).[434]

There is limited knowledge of, and transparency in the development of the centralised APIs. The participation of volunteers and their mandates was also decided behind closed doors as India Stack is neither bound by procurement prohibitions nor are their actions auditable. This arrangement means India Stack operates without the same degree of oversight mandated by similar government projects.

A winner-takes-all strategy is in play where first-mover advantage is used to expand services aggressively across several important sectors. These services and products are framed as voluntary solutions that lower costs and improve innovation, efficiency and consumer choice. The state mandates their use by consumers and integrates them into different aspects of the digital economy. As these services scale, network effects increase switching costs and create consumer dependence.

Aadhaar, UPI, Digital Locker and DEPA mediate critical functions associated with the digital economy. For Aadhaar, Account Aggregator and DEPA, the technical infrastructure is owned and operated by the public-private consortiums. The key policy considerations associated with India Stack are defined by actors and bodies invested in the development of its services and frameworks. This includes its developers, implementing agencies, creators of proprietary sub-APIs, investors, and custodians. Agencies and businesses that stand to generate profits through India Stack, are also integrated in the maintenance of the critical digital infrastructure.

In India, the concentration of power and the state backing allows institutions and platforms associated with India Stack to leverage that scale more effectively than any other private market player. Network effects and consolidated infrastructural power grant institutions like UIDAI and NPCI an unmatched ability to control data and market access, set terms for revenue generation and constrain competition.

Markets with India Stack solutions are characterised by lack of competition and high-barriers to entry. The existence of Aadhaar outside of a legislative mandate and its rampant adoption and brazen expansion despite Supreme Court orders are evidence of the oligopolistic power of these institutions. Unlike classic monopoly power, state and market collaboration enable these institutions to amass enormous control over institutional partners, service providers and consumers on either side of the market.

Aadhaar structures online identity verification for vast numbers of consumers and service providers. The UPI dominates consumers seeking the ease of online mobile payments, banking and financial service providers, and merchants. UIDAI and NPCI and by extension the state have also secured control over critical aspects of data flows, often rationalised and defended on grounds of national security and consumer interests. The ability of the RBI to continue to subsidise UPI and UIDAI's push to allow private companies to use Aadhaar demonstrates the advantages of strong oligopolies and a captive consumer base.

A large consumer base also enables India Stack to evade regulation and negotiate with both the market and the state. As demonstrated with Aadhaar, the state used mandatory-voluntary mandates to embed the digital identity in citizens lives, which enabled UIDAI to build a defence of 'too-big-to-fail' to tilt policy makers in its favour. The current Finance Ministry has allowed 22 financial companies, operating under the PMLA, to verify the identity of clients and beneficiaries using their Aadhaar numbers and Aadhaar-based authentication.[435]

The Indian government has been using its ability to shape the actions of its population and private sector to determine which technologies and technological architecture are adopted domestically. While there are market alternatives to the commercial platforms that India Stack compares itself to, such as Google Maps, most India Stack solutions are integrated into the digital economy in such a way that consumers are locked in. If citizens or companies want to operate in a digital economy they must or will inevitably end up engaging with its architecture.

India Stack is an industry and state backed initiative that has leveraged India's massive population, its large domestic market and huge domestic demand potential, to create a captive consumer base and achieve market dominance. An increase in the scale of transactions using solutions developed by India Stack makes the model viable and creates opportunities for the state to seek alternative investment options. This is demonstrated in efforts of the Indian government to export India Stack, pitching it as a globally competitive model and “a cost-effective innovation and data democratisation tool that allow… access to high-quality, authentic data without spending a massive amount of money…while maintaining data security.”[436]

As the promoters of India Stack seek its adoption beyond India, it is difficult to imagine achieving such network effects without a permissive political and legal landscape. India not only lacks a data protection law but parliamentary, institutional and legal arrangements have been subverted to push through adoption of India Stack solutions. While consumer dependence has been used to legitimise business models and seek regulatory leeway, basic consumer protection measures like grievance redressal are lacking. It would have been better if data-driven solutions of the India stack operate as purely market interventions as they have proven to be more adept at accommodating consumer needs.

India Stack is as much a product of natural and technological changes as it is of India's sovereignty based approach to governance of data. Its emergence is rooted in digital neomercantilism - where India defines national security in terms of the state gaining control over writing the rules for the economy, technology, and finance. Giving geo-politics the leading role conflicts with domestic agendas of economic, social growth and development.

India Stack has expanded state-market collaboration where in addition to outsourcing the development of technology products and services to the private-sector, the government is outsourcing key governance functions like regulation and policy development to entities like UIDAI and NPCI. The rise of India Stack has been led by the state through political-institutional structures and regulatory policies. While public-private collaboration is politically powerful, there must be an independent audit to measure costs and benefits of backing India Stack.

While India Stack is succeeding at building at scale, integrating the services developed under its umbrella into different kinds of social governance processes carries significant political and socio-economic consequences. Provisioning of public goods and infrastructure should be held to a higher standard of accountability and trust. If India Stack wants to lay claim to these labels then it must take on associated responsibility and the state must ensure accountability.

India Stack institutionalises the regulations, standards, conventions, and processes associated with data collection and use in India. The architecture of India Stack has influenced the enterprises, conventions and practices emerging from its fold. India Stack is better understood as a recalibration of the state's approach to governance of data, a mechanism to extend control sometimes by enabling accumulation and sometimes by restricting access to data from important markets. India's efforts to extend sovereignty over data, however, have consequences for innovation, competition and consumer protection. As India Stack expands and more components are added, regulation for protection of data and competition need to evolve in tandem.

GT

Internet
Governance
Project

📍 D. M. Smith Building, 685 Cherry Street,
Atlanta, GA 30332-0345

☎ 404.385.8577

📠 404.385.0504

🌐 www.internetgovernance.org

A Unit of the University System of Georgia
An Equal Education and Employment Opportunity Institution

Endnotes

01 Ministry of Finance, Economic Survey 2022-23: Highlights, 31 January 2023

02 Newzoo.Global Mobile Market Report 2021; Top Countries by Smartphone Users. 2023.

03 Economic Survey of India 2021-22, Chapter Industry and Infrastructure

04 Data.ai, State of Mobile 2022

05 Business Today, By 2025, there'll be more Internet users in rural India than urban areas: report, June, 2021

06 Sadowski, J. When data is capital: Datafication, accumulation, and extraction, Big Data and Society, January-June 2019

07 Mueller, M. A Critique of the 'Surveillance Capitalism' Thesis: Toward a Digital Political Economy August, 2022. Kuerbis, B., & Mueller M., Exploring the role of data enclosure in the digital political economy 2022. Workshop on the Economics of Information Security. Zuboff, S. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs, 2019. Athique A., Parthasarathi V. & Srinivas S. (eds)., The Indian Media Economy (2-volume set) Vol. I: Industrial Dynamics and Cultural Adaptation Vol. II: Market Dynamics and Social Transactions, India: Oxford University Press, 2017. Srnicek N, Platform Capitalism, Cambridge: Polity Press, 2016.Khera, R. Dissent on Aadhaar: Big Data Meets Big Brother, Orient BlackSwan

08 Boyd D, Crawford K (2012) Critical questions for Big Data: Provocations for a cultural, technological and scholarly phenomenon. *Information*, Communication & Society 15(5): 662–679. Panday, J. and Malcolm, J. The political economy of data localization, The Open Journal of Sociopolitical Studies, Partecipazione e Conflitto, 2018. Panday J. Data Protection as a Social Value, Economic and Political Weekly Vol. 52, No. 51 (DECEMBER 23, 2017), pp. 62-65 (4 pages)

09 Mueller, M. L., and Farhat, K. Regulation of platform market access by the United States and China: Neo-mercantilism in digital services. *Policy & Internet. 2022*

10 Blumenthal, R., Schatz, B., Wyden, R., Lujan, B., Markey, E., Klobuchar, A., Booker, C., Warren, E., and Coons, C. "Letter to FTC Chairperson Lina Khan," 20 September, 2021,

11 The White House, Fact Sheet: Biden-Harris Administration Announces New Initiative to Improve Supply Chain Data Flow, 15 March 2022
The White House, FACT SHEET: Biden-Harris Administration Releases Recommendations for Advancing Use of Equitable Data, 22 April 2022
The White House, Executive Order on Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security, 27 March 2023

12 Jinhe Liu, J. China's data localization, Chinese Journal of Communication, 2020, Vol. 13, No. 1, 84–103

13 Testimony by Peter Swire, U.S. Senate Commerce Committee Hearing "The Invalidation of the EU-U.S. Privacy Shield and the Future of Transatlantic Data Flows", 9 December, 2020

14 European Commission, The Digital Services Act package

[15] European Commission, European Data Governance Act

[16] Julia Pohle, J. and Thiel, T. Digital sovereignty, Internet Policy Review, Volume 9, Issue 4, 17 December, 2020.

[17] Supra Note (Pohle 2020)

[18] Chander, A. and Lê, U. Data Nationalism, Emory Law Journal, Volume 64, Issue 3. 2015

[19] Mueller M. "Against Sovereignty in Cyberspace," International Studies Review, Volume 22, Issue 4. 2020

[20] Mueller M. Digital sovereignty: What does it mean? UN Internet Governance Forum, 2021

[21] India Stack

[22] India Brand Equity Foundation (IBEF), A Public Digital Infrastructure, India Adda-Perspectives on India, 27 January, 2023

[23] Shah, V. and Nilekani, N. Rebooting India: Realizing a billion aspirations, Penguin Books, 2015

[24] NASSCOM, Digital India: Digital Public Goods Platformisation Play

[25] Nandan Nilekani on Data Empowerment and the 'Opportunity' State, IDFC Institute Dialogues August 2018

[26] Chatterjee, A. UPI to Aadhaar, Modi govt showcases 'India Stack' of digital goodies for global adoption, The Print, 23 January, 2023

[27] Adhia, N. The History of Economic Development in India since Independence, India: Past, Present, and Future, Volume 20, 2015

[28] Established in 1976 with 4.4 million United States Dollar (USD) in financial assistance from the United Nations Development Programme (UNDP). National Informatics Centre, Organization, Functions and Duties

[29] World Bank, India: An Industrializing Economy in Transition. A World Bank Country Study. December. 1989

[30] Heeks, R. Import Liberalization and Development of Indian Computer Industry, Economic and Political Weekly, 26 August 1995

[31] A survey by NASSCOM indicates that in 1998-99, more than 200 of Fortune 1000 companies outsourced their software requirements from India.Nasscom on Indian software industry news, Domain-b, 20 August 1999

[32] Chandana Chakraborty and Dilip Dutta, Indian Software Industry: Growth Patterns, Constraints and Government Initiatives, 2002

[33] India's total software exports grew from USD 734 million in 1995-96 to USD 4 billion in 1999-2000. Chandana Chakraborty and Dilip Dutta, Indian Software Industry: Growth Patterns, Constraints and Government Initiatives, 2002

[34] The Telecom Regulatory Authority of India Act, 1997

[35] Vasudha Venugopal, Swadeshi Jagran Manch welcomes curbs on 'predatory behavior', The Economic Times, 28 December, 2018. Two-day coordination meeting of BJP, RSS to begin today, Hindustan Times, 19 October, 2021

[36] Swaminathan S. Anklesaria Aiyar, India's New Protectionism Threatens Gains from Economic Reform, Cato Institute, 18 October 2018

[37] Shri Yashwant Sinha, Minister of Finance, Speech Introducing the Budget for the year 1999-2000.

[38] List of Council of Ministers as on 30 January 1999. UPA-I continued with the Ministry of Information & Broadcasting but the Ministry of Communications was reformulated as the Ministry of communications and information technology (MCIT). The department of Electronics was shifted from under the PM to the MCIT.

[39] The National Population Register (NPR) is a Register of usual residents of the country. It is being prepared at the local (Village/sub-Town), sub-District, District, State and National level under provisions of the Citizenship Act 1955 and the Citizenship (Registration of Citizens and issue of National Identity Cards) Rules, 2003. R. Ramakumar, What the UID conceals, The Hindu, 21 October, 2010

[40] Members of the Council of Ministers sworn in on 22 May, 2004

[41] National Knowledge Commission, Report to the Nation, 2006-09

[42] Ibid

[43] National Knowledge Commission, Recommendations on e-Governance 20 November, 2008

[44] Data Centres, State Wide Area Networks (SWANs)

[45] The UPA government allocated Rs 600 crores, a matching amount was allocated by the Planning Commission. S. Sadagopan, e-governance: A long way to go, The Economic Times, 11 February 2006

[46] These include Bhoomi (land record management in Karnataka), Akshaya (IT literacy and local entrepreneurship in Kerala), Khajane (treasury network in Karnataka), Gyandoot (ICT to boost village level entrepreneurship in MP), e-Seva (single window access to many government services in Andhra Pradesh), SARI (Sustainable Access in Rural India in Tamil Nadu), and Honey-bee Network (knowledge centers for local knowledge in Gujarat).

[47] The Department of Telecommunications (DoT), the Telecommunication Engineering Center (TEC) in consultation with security agencies

[48] Anand Sinha, Changing Contours of Global Crisis – Impact on Indian Economy, Reserve Bank of India, 2012

[49] Ministry of Communications and Information Technology, Legal Framework For Mandatory Electronic Delivery of Services, 02 December, 2012

[50] Ministry of Finance, Department of Economic Affairs, Technology Advisory Group for Unique Projects (TAG-UP) - Constitution and Terms of Reference, 1 June 2010

[51] Jain, R. 'The Indian broadband plan: A review and implications for theory', Telecommunications Policy Volume 38, Issue 3, April 2014, Pages 278-290

[52] The All India Trinamool Congress (AITMC) is an Indian political party active mainly in West Bengal and Goa.

[53] India Today, FDI debate begins, BJP says government went back on promise, 4 December 2012

[54] US represented 37% of the global market for IT goods and services in 2005 but had shrunk to 33% share in 2008

[55] Nayan Dave, Gloom a boom for Gujarat IT exports. The Economic Times, 19 January 2010

[56] Ministry of Finance, Department of Economic Affairs Mid-Year Economic Analysis 2014-2015,

[57] Rohin Dharmakumar and N.S. Ramnath, Is ISpirt An Alternative To Nasscom? Forbes India, 20 February, 2013

[58] Ibid footnote 176

[59] Rohin Dharmakumar, Platform ambitions: The story of how iSpirt lost its true north, The Ken, 21 September, 2017

[60] Sixth BRICS Summit – Fortaleza Declaration 15 July, 2014

[61] Government of India's Initial Submission to Global Multistakeholder Meeting on the Future of Internet Governance; Sao Paulo, Brazil on April 23-24, 2014.

[62] Indian Government Declares Support for Multistakeholder Model of Internet Governance at ICANN 53, 22 June 2015

[63] Richard M. Rossow, India's FDI Reforms Under Modi: Once a Fountain, Now a Drip, 2017

[64] A new government Ministry and agency was established to refinance loans to and advocate the cause of micro, small, and medium-sized enterprises (MSMEs).

[65] Ministry Of Electronics & Information Technology, Government Of India, India's Trillion Dollar Digital Opportunity

[66] Make in India. Salman SH, Budget 2017-18: What It Means For Electronics Manufacturing, Medianama, 1 February 1, 2017

[67] Vivek Pai, DeitY Envisaged 'Digital India' Gets A Nod From The Cabinet, Medinama, 21 August, 2014.

[68] National Optical Fiber Network launched in 2011 was rebranded under two separate programs BharatNet, a program to provide Internet access to all villages in the country. Digital India, Bharat Broadband Network (BBN) and Universal Access to Mobile a program designed to provide mobile connectivity to over 55,000 villages Digital India, Universal Access to Mobile Connectivity

[69] An initial sum of INR 2510 crore was allocated in the 2015-2016 budget for policies around connectivity, skilling and digital governance under the program.

[70] StartUp India was a one-stop platform for all stakeholders in the Startup ecosystem to interact amongst each other

[71] Launched in 2015, with the key objective of promoting cities to provide core infrastructure, a clean and sustainable environment and a decent quality of life for citizens through the application of 'smart solutions'. Indian Ministry of Housing and Urban Affairs Smart Cities: Vision.

[72] Shaju Philip, Kochi underway, PM Modi says 50 cities ready for Metro, The Indian Express, 1 June 2017

[73] Hindustan Times, Govt withdraws plan to create social media hub after Supreme Court's 'surveillance state' remark, 3 August 2018

[74] NDTV, Watch: The Moment PM Modi Announced 500 and 1,000 Rupee Notes Are Illegal, 8 November, 2016

[75] Department of Telecom, National Digital Communications Policy 2018

[76] Sectors like insurance, retail trade, defence, private security, pensions, FM radio, uplinking television channels, and print media.

[77] Department of Industrial Policy and Promotion, Ministry of Commerce and Industry (DIPP), Press Note 2 of 2018 (PN 2) 26 December, 2018

[78] Data localisation mandates for financial data, personal and non-personal data covered below

[79] PM Modi bats for self-reliance in technology sector, LiveMint, 02 March, 2022

[80] Speech of Arun Jaitley, Minister of Finance, Budget 2018-2019, 1 February, 2018

[81] Himanshu, India's slow but sure de-industrialisation is worrying, LiveMint, 15 June 2023

[82] Ministry of Electronics & Information Technology (e-Governance Division), Draft Data Centre Policy 2020

[83] Cabinet approves Programme for Development of Semiconductors and Display Manufacturing Ecosystem in India, 15 Decmber 2021

[84] Department of Commerce, Secretary Raimondo Announces U.S.-India Semiconductor Supply Chain and Innovation Partnership MOU in New Delhi, 15 March, 2023

[85] Reserve Bank of India, Survey on Computer Software and Information Technology Enabled Services Exports: 2021-22, 8 September, 2022

[86] Deepak Mishra, D. et al. State of India's Digital Economy, Indian Council for Research on International Economic Relations (ICRIER) Prosus, Center for Internet and Digital Economy, February 2023

[87] Broadcast Engineering Consultants India Limited (BECIL), Invitation for Expression of Interest for empanelment of agency for Monitoring and Response Management Services related to 24 x 7 function, operation and maintenance of Social Media Communication Hub of different Ministries/Govt. organisations, 24 October, 2019

[88] Pankaj Doval, Twitter executives could face 7-year jail, warns government, Hindustan Tmes, 13 March 2019

[89] Ministry of Electronics and Information Technology (MeitY), 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 & Trusted Internet", 28 April, 2022

[90] Business Standard, India ranks 2nd in total number of data breaches exposed in 2022: Report, 1 March 2023

[91] Ministry of Electronics and Information Technology (MeitY), Cybersecurity Attacks, Rajya Sabha Unstarred Question No. 1043, Answered on 10 February 2023

[92] Indian Ministry of Electronics and Information Technology, "India's Trillion-Dollar Digital Opportunity" 2019

[93] P Hebbar, 5 Instances Where PM Narendra Modi Championed The Power Of Data, Analytics India Magazine, September 2019. HT Correspondent, 'Data is the new oil, new gold,' says PM Modi in Houston, The Hindustan Times, 23 September, 2019.

[94] Indian Ministry of Finance, "Data 'of the People by the People, for the People," in Economic Survey 2018–2019. 78–97

[95] Sengupta, D. and Aulakh, G. Data belonging to Indians must reside within the country, says Aruna Sundararajan, The Economic Times, 30 July, 2018

[96] Data is integral to Digital India: Amitabh Kant, ET Telecom, 2 December, 2021

[97] The Digital Personal Data Protection Bill, 2022

[98] Krishnadas Rajgopal, K. New Digital Personal Data Protection Bill in Monsoon Session, The Hindu, 12 April 2023

[99] Non personal data, according to the report, could be either factual data or analysis, which has been stripped of any personal identifiers.

[100] Ministry of Electronics and Information Technology (MeitY), National Data Governance Framework Policy, May 2022

[101] Trisha Jalan, "Data Localisation, Digital Nationalism Need Of The Hour, Says Swadeshi Jagran Manch To PM: Reports," Medianama, 9 December, 2019

[102] Soumyarendra Barik, Data A 'National Resource', Confident The Govt Will Introduce 'Sound' Data Regulation Framework To Protect It: Mukesh Ambani, Medianama, 6 October, 2020. Punj, S. India Today Conclave 2017: Mukesh Ambani pitches for 'keep in India'." India Today. 2017

[103] Nandan Nilekani, Why India needs to be a data democracy, LiveMint, 27 July, 2017

[104] India boycotts Osaka Track at G20 Summit, LiveMint, 30 June, 2019

[105] Suhasini Haidar, "At G20, India stands with developing world — not U.S., Japan — on 5G and data," The Hindu, June 28, 2019. See also Jennifer Daskal and Justin Sherman, Data Nationalism on the Rise: The Global Push for State Control of Data, June 2020

[106] Couldry, N. and Meijas, U. Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject
Special Issue: Big Data from the South, Sage Publications Volume 20, Issue 4

[107] Sharma R. IndiaTV, There can be no compromise on India's digital sovereignty: Ravi Shankar Prasad

[108] Mathur, V. What is Data Colonization, And Why we in India Need to Rework The Policies in Place, News18, 21 January, 2019. Reliance Industries Ltd. is the sole beneficiary of Independent Media Trust which controls Network18 Media & Investments Ltd.

[109] Data colonisation the new looming danger, CNBC TV18, 27 June, 2019. Mukesh Ambani says 'data colonisation' as bad as physical colonisation, The Economic Times, 19 December, 2019

[110] Smriti Parsheera, An Analysis of India's New Data Empowerment Architecture, Emerging Trends in Data Governance, Edited by Swati Punia, Shashank Mohan, Jhalak M. Kakkar, and Vrinda Bhandari, 2023

[111] Bilal Mohamed, Fiduciary relationships and the feasibility of data trusts to address asymmetries in the data economy, The Data Economy Lab, 20 November, 2021
Trishi Jindal and Aniruddh Nigam, Data Stewardship for Non-Personal Data in India - A Position Paper on Data Trusts, Vidhi Centre for Legal Policy, November 2020

[112]

Report of the Group of Experts on Privacy - Chaired by Justice A P Shah, Former Chief Justice, Delhi High Court, Planning Commission of the Government of India, 16 October, 2012

[113] India can offer a radically new way of looking at data: Nandan Nilekani, The Print, 9 August, 2018

[114] Siddharth Tiwari, Frank Packer, and Rahul Matthan, Data by People, for People, International Monetary Fund, March 2023

[115] The Justice Srikrishna Committee Report, the Bill introduced in Parliament in 2019, the Joint Parliamentary Committee version of the Bill from late 2021 and the recent government draft put out for consultation in 2022 represent the constantly evolving approach. The Personal Data Protection Bill, July 2019 stipulated that "sensitive personal data" can be processed and transferred outside India only with the explicit consent of the data principal, and as long as the country meets certain safeguards. This bill that since been withdrawn by the government. The local data storage requirements for categories of data deemed important or strategic cover a range of largely commercial services.

[116] Department of Industrial Policy and Promotion, Ministry of Commerce and Industry, Government of India, Consolidated FDI Policy, 2017 Annexure

[117] Aditi Agrawal, "Cyber Attacks On Critical Infrastructure Increased During Pandemic: Ajit Doval", Medianama, September, 2020

[118] PM Modi says self-reliance in technology will create jobs in country, Business Standard, 3 March, 2022

[119] Shruti Dhapola, More Chinese apps banned in India: Lack of transparency is worrying, say experts, Indian Express, 20 Nov, 2020. Press Information Bureau. 2020. "Government Bans 59 mobile apps which are prejudicial to sovereignty and integrity of India, defense of India, security of state and public order." Accessed 15 December 2020.

[120] Indian Express, Govt blocks 14 mobile apps on terror suspicion, 2 May 2023

[121] Ministry of Electronics and Information Technology (MeitY), 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 & Trusted Internet, No. 20(3)/2022-CERT-In, 28 April, 2022. This would require data centers, virtual private server (VPS) providers, cloud service providers, and virtual private network (VPN) providers to register and maintain the names of customers and subscribers, period of hire, IP addresses allotted to or used by customers, email address and IP address and time stamp at the time of registration, purpose of hiring such services, validated address and contact numbers, and the ownership patterns of subscribers for a period of five years, even after the cancellation or withdrawal of such subscription.

[122] Xinmei Shen, Chinese data exchange makes first sale involving personal data, paving the way for jobseekers to profit from their resumes, South China Morning Post, 2 May 2023

[123] Economic Survey 2018-19. In economic theory, public goods possess two specific qualities: they are non-exclusive (anyone can have access to them), and 'non-rivalrous' in consumption (i.e. their use does not deplete their availability for use by others). Data can meet both conditions, though exclusion is possible.

[124] Draft e-commerce policy says data is a national asset, compares it to mine of natural resources, Scroll.in, 24 February, 2019

[125] Department of Promotion of Industry and Internal Trade's (DPIIT), Draft National e-Commerce Policy India's Data for India's Development, 23 February 2019

[126] National Data Governance Policy Framework (NDGPF), May 2022

[127] Shri Rajeev Chandrasekhar, The Minister of State for Electronics & Information Technology, in a written reply to a question in Lok Sabha on the National Data Governance Framework Policy, 27 July 2022

[128] Report by the Committee of Experts on Non-Personal Data Governance Framework

[129] A community is defined in the report as any group of persons bound by common social or economic ties, territorial parameters, or another interest or purpose.

[130] Nikhil Pahwa, India Must Avoid Nationalization Of Data, Medianama, 25 July, 2020

[131] Supra note Economic Survey 2018-2, 4.37, Page 90.

[132] The card was a microprocessor chip with a memory of 16 KB linked to 16 fields establishing the identity of the individual ranging from personal details, photographs and finger biometry and a unique identification number. The National Population Register (NPR) is a Register of usual residents of the country. It is being prepared at the local (Village/sub-Town), sub-District, District, State and National level under provisions of the Citizenship Act 1955 and the Citizenship (Registration of Citizens and issue of National Identity Cards) Rules, 2003. R. Ramakumar, What the UID conceals, The Hindu, 21 October, 2010

[133] Selected sub-districts of Andhra Pradesh, Assam, Goa, Gujarat, Jammu and Kashmir, Rajasthan, Tripura, Uttar Pradesh, Uttarakhand, Tamil Nadu, West Bengal and Puducherry.

[134] E-seva introduced passport services for application and renewal of Passports, PAN card application services. The Mint, "The changing faces of public service delivery systems", December 9, 2010.

[135] Pandey, Priyanka. "Service delivery and corruption in public services: How does history matter?. " *American Economic Journal:* Applied Economics 2, no. 3 (2010): 190-204

[136] Department of Food and Public Distribution, the Ministry of Consumer Affairs, Food and Public Distribution, Highlights, 3 November, 2003

[137] E-seva introduced passport services for application and renewal of Passports, PAN card application services. The Mint, "The changing faces of public service delivery systems", December 9, 2010.

[138] Written Response of Akhilesh Prasad Singh, Consumer Affairs, Food and Public Distribution to Sanjay Raut, Question on Smart Card System, Rajya Sabha, Session 202, 20 August 2004

[139] Department of Information Technology, Ministry of Communications and Information Technology, Government of India approved the Unique Identification for BPL Families project 3 March 2006

[140] 'The creation of the strategic vision document is acknowledged by the UIDAI on its website but this document has not been shared with the public. Gopal Krishna, Where Is WIPRO's "Strategic Vision On The UIDAI Project" Document?, Countercurrents.org, 7 August, 2011.

[141] The Empowered Group of Ministers (EGoM) set up on 4 December, 2006 was composed of the then Ministers of External Affairs, Home Affairs, Law, Panchayati Raj and Communications and Information Technology and the then Deputy Chairman, Planning Commission.

[142] Planning Commision of India, Notification for formation of UIDAI, 28 January, 2009. Gazette Notification No.-A-43011/02/2009-Admn.

[143] Press release for appointment of Nilekani as chairman of UIDAI, 2009.

[144] Key appointments included Pramod Varma as Chief Architect and Technology Advisor, Regunath Balasubramaniam as Principal Architect UID, Srikanth Nadhamuni as Head of Technology and Sanjay Jain as Chief Product Manager. Usha Ramanathan, Aadhaar From Welfare to Profit, Dissent on Aadhaar: Big Data Meets Big Brother, edited by Reetika Khera, Orient BlackSwan, 2019

[145] The PM Council was established on 30 July 2009 and substituted by a Cabinet Committee on 22 October 2009

[146] Hari Tn & Hari Menon, The man who rang in a new era in India's telecom sector, YS Journal, 28 September 2018

[147] UIDAI, Strategy Overview: Creating a Unique Identity for Every Resident in India, April 2010

[148] It created a process of "seeding" or integrating the UID number with other records of the residents in public or private databases. UIDAI, Standard Protocol Covering the Approach & Process for Seeding Aadhaar Numbers in Service Delivery Databases. June 2015.

[149] UIDAI, Aadhaar enrollment.

[150] Common Service Centers (CSC) are bodies authorised by the central government to manage enrollment, updates and correction in Aadhaar. CSCs were introduced under the National e-Governance Plan, the implementation of which was funded by financial contributions from Infosys and Wipro founders amongst others.

[151] Pratyush Ranjan Tiwari et al., India's "Aadhaar" Biometric ID: Structure, Security, and Vulnerabilities, 2022

[152] Unique Identification Authority of India (UIDAI), 'Aadhaar Technology and Architecture', 2014

[153] Unique Identification Authority of India (UIDAI), Authentication Ecosystem
Unique Identification Authority of India (UIDAI) Aadhaar e-KYC API 1.0 (Final), May 2016

[154] Unique Identification Authority of India (UIDAI), QR Code Reader, Authentication Devices & Documents
Unique Identification Authority of India (UIDAI), Aadhaar Paperless offline e-KYC

[155] Open Source, Aadhaar: A Testimony to Success of FOSS in India!, 4 December, 2011.

[156] Usha Ramanathan, Aadhaar Unmasked ~ What we (don't) know about the companies, The Statesman, 12 July 2013

[157] Jyoti Panday, Electronic Frontier Foundation, Aadhaar: Ushering in a Commercialized Era of Surveillance in India, 1 June, 2017.

[158] L-1 Selected as Biometric Provider for Indian Unique Identification Program, ASMag.com, 28 July, 2010. IBM, HP opt out of 2,000-crore UIDAI bid, The Economic Times, 17 May, 2011

[159] With a crucial role in the UID programme, 4G Identity Solutions steps into big league, The Economic Times, 13 August 2010.

[160] Harsimran Julka, HCL Infosystems wins Aadhaar contract of Rs 2,200 crore from UIDAI, The Economic Times, 2 Mach 2012. Mahindra Satyam and Morpho Biometric Solutions Deployed by Indian Identification Authority, ASMag.com, 2 August, 2010

[161] Accenture Newsroom, UIDAI Selects Accenture to Implement a Multimodal Biometric Solution for "Aadhaar" Program, July 2010. Giving 1.2 billion citizens a unique identity, 2010 LTIMindtree Insights.

[162] Standing Committee on Finance (2011-12), Report on the The National identification Authority of India Bill, 2010, 2011

[163] Reserve Bank of India, Guidelines for the issue of Smart / Debit Cards by banks, 12 November, 1999 IBS Center for Management Research, The Indian Internet Banking Journey, Case Study: ICICI - Internet Banking Initiatives, 2010

[164] Reserve Bank of India, Draft Guidelines for issuance and operation of Prepaid Payment Instruments in India.

[165] Oxigen launched in 2004. FirstPost, Wallet365.com launched by TimesofMoney, TimesofMoney a subsidiary of the media firm Times Group and YES Bank collaborated to launch Wallet365 in 2006. Mobikwik launched in 2009. Paytm was launched as a prepaid mobile and DTH (direct-to-home) recharge platform in 2010 but later expanded into a full-fledged digital wallet

[166] Reserve Bank of India, Internet Banking in India – Guidelines, 14 June, 2001 Internet Banking in India – Guidelines 20 July, 2005

[167] Reserve Bank of India, RBI introducing Special Electronic Funds Transfer, 31 March, 2003.

[168] RTGS Services now for Bank Customers: RBI, 2004

[169] Reserve Bank of India, NEFT System goes live, 21 November, 2005

[170] BIS, 'Central banks and payments in the digital era', (BIS Annual Economic Report, 2020)

[171] Section 58(2)(p) and 58(2)(pp)

[172] Memorandum Committee on Payment Systems (headed by Dr. R H Patil, Chairman, The Clearing Corporation of India Ltd) 16 July, 2002. The draft regulation broadly covered the powers of the RBI for regulation of payment systems, provision of legal basis for clearing and netting of settlements and RBI's powers to frame regulations.

[173] CPSS, BIS, 'A glossary of terms used in payments and settlement systems

[174] In addition to the RTGS the committee had recommended that the Interbank Clearing System, the High Value Clearing System, the Securities Clearing and Settlement System, the MICR Clearing System, the proposed Government Securities and Foreign Exchange Clearing Systems be classified as SIPS.

[175] Payment and Settlement Systems Act 2007 (PSS Act)

[176] The same is sought to be covered through the "Oversight Framework for Financial Market Infrastructures (FMIs) and Retail Payment Systems (RPSs)" 13 June 2020

[177] Section 10 and section 18

[178] Willem H. Buiter, Negative Nominal Interest Rates: Three Ways to overcome the Zero Lower Bound, National Bureau of Economic Research, Working Paper 15118, June 2009

[179] The study for the Indian banking sector for the period 2005-06 to 2009-10 too suggested efficiency gains resulting from technological innovations and investment in IT. Rajput, N. and M. Gupta (2011), "Impact of IT on Indian Commercial Banking Industry: DEA Analysis", Global Journal of Enterprise Information System, 3(1).

[180] Ministry of Finance, Recommendations of the Committee on Financial Inclusion, 5 February, 2008

[181] Financial services include credit, savings, insurance and payments and remittance facilities

[182] The Financial Inclusion Promotion & Development Fund and the Financial Inclusion Technology Fund

[183] Ibid 206 RBI Vision 2012-2015

[184] NPCI Background

[185] National Financial Switch (NFS) a network of 50,000 ATM maintained by 37 member banks was taken over by NPCI on December 14, 2009.

[186] NPCI launched IMPS on 22 November 2010

[187] NPCI launched RuPay in 2012

[188] Indian Bankers Association, UIDAI, IRDBT, NPCI, "Micro-ATM Standards" March, 2010.

[189] UIDAI Strategy Overview, April 2010, https://archive.org/stream/StrategyOverveiw001/Strategy_Overveiw-001_djvu.txt

[190] Aadhaar-enabled Payment System

[191] Terms of Reference of Task Force for Direct Transfer of Subsidies 14 February, 2011

[192] Report of the Task Force on an Aadhaar-Enabled Unified Payment Infrastructure, February 2012

[193] Banking Correspondents (BCs) are networks of intermediaries engaged by banks as their proxy to provide banking services at under served or unserved regions.

[194] Committee on Payment and Settlement Systems (CPSS) was renamed and reconfigured to become the Committee on Payments and Market Infrastructures (CPMI) in 2014. CPMI also serves as a forum for central bank cooperation in related oversight, policy and operational matters, including the provision of central bank services. The Reserve Bank of India is a member.

[195] The Working Group on Innovations in Retail Payments was set up by the Committee on Payment and Settlement Systems (CPSS) to provide an overview of innovative retail payment activities in CPSS and other select countries over the past decade.

[196] BIS (2012), Innovations in Retail Payments – A Report, CPSS, Basel

[197] Report on Trend and Progress of Banking in India 2012-13. Submitted to the Central Government in terms of Section 36(2) of the Banking Regulation Act, 1949.

[198] Prepaid payment instruments are issued by non-banks to be used for the payment of goods and services over the Internet and mobile network. Cash withdrawal and funds transfer between instruments were not permitted and prepaid funds are to be kept in an escrow account at a bank. Security features include limits for the maximum loading amount, limits for individual transactions, and a validity period.

[199] Background Note on Introduction to Cash Transfers, prepared National Committee on Direct Cash Transfers

[200] Privacy Activist Usha Ramanathan On How Aadhaar Has Taken Over Our Lives, Huffington Post, 25 September 2019

[201] W.P(C) No. 439 of 2012 titled S. Raju v. Govt. of India and Others pending before the D.B. of the High Court of Judicature at Madras and PIL No. 10 of 2012 titled Vickram Crishna and Others v. UIDAI and Others pending before the High Court of Judicature at Bombay were transferred to the Supreme Court vide Order dated September 23, 2013. Also W.P. No. 833 of 2013 titled Aruna Roy & Anr Vs Union of India & Ors, W.P. No. 829 of 2013 titled S G Vombatkere & Anr Vs Union of India & Ors and Petition(s) for Special Leave to Appeal (Crl) No(s).2524/2014 titled Unique Identification Authority of India & another v. Central Bureau of Investigation.

[202] Constitutionality of Aadhaar Act, Justice K.S. Puttaswamy v Union of India, SCC Observer, 2012-2017

[203] Nikhil Pahwa, West Bengal Assembly Passes Resolution Asking Aadhaar To Be Delinked From LPG Subsidy, Medianama 3 December 2013

[204] Supreme Court of India, WRIT PETITION (CIVIL) NO.494 OF 2012

[205] The WIre, Timeline: Twenty Two Mandatory Notifications for 'Voluntary' Aadhaar Since January 2017, March 09, 2017

[206] Reserve Bank of India, Payment Systems in India: Vision 2012-15, 1 October 2012

[207] Ibid.

[208] Ibid.

[209] Slogan of bijli, sadak, pani is passé: Nilekani, Hindustan Times 14 February 2010

[210] Reetika Khera, UID: from inclusion to exclusion https://india-seminar.com/2015/672/672_reetika_khera.htm

[211] Suranjana Roy, Komal Gupta, The Livemint, Welfare schemes for which aadhaar is mandatory, March 8th, 2017.

[212] Reetika Khera, Lessons from the East Godavari pilot, The Hindu, 11 April, 2013

[213] Know Your Customer Norms – Letter issued by Unique Identification Authority of India (UIDAI) containing details of name, address and Aadhaar number, 2011. Securities and Exchanges Board of India (SEBI) Know Your Client Requirements. 8 October 2013. IRDAI, FAQ on Insurance Repository, 2013.

[214] Launched in December 2012 National Automated Clearing House Product Overview - NACH

[215] Launched in November 2012 only two state owned telecom service providers MTNL & BSNL offered the service.

[216] Zero balance and zero charges" basic savings bank deposit (BSBD) accounts. Allows minimal paperwork, relaxed KYC, e-KYC, account to be opened in camp mode

[217] Economic Survey of India, 2015 Chapter 3, 'Wiping every tear from every eye': the JAM Number Trinity Solution

[218] PM Narendra Modi open to radical ideas: Nandan Nilekani Times of India, May 17, 2022

[219] Pradhan Mantri Jan Dhan Yojana (PMJDY), launched by the Prime Minister Narendra Modi on 28th August, 2014

[220] Vivek Pai, 10 Cr Aadhaar cards linked to bank accounts: Planning Commission. Medianama, 14 December, 2014.

[221] Securing the Unsecured pertains to issuance of indigenous debit cards for cash withdrawals and payments at merchant locations.

[222] including a savings account, remittance, credit, insurance, and pension

[223] Funding the Unfunded pertains to other financial products like micro-insurance, overdraft for consumption, micro-pension and micro-credit

[224] Revised the Allocation of Business Rules to attach UIDAI to Department of Electronics & Information Technology (DeitY) in 12 September 2015

[225] The Attorney General argued that the Constitution's framers never intended to incorporate a right to privacy, and therefore, to read such a right as intrinsic to under Article 21, or to the rights to various freedoms (such as the freedom of expression) guaranteed under Article 19, would amount to rewriting the Constitution.The government also pleaded that privacy was "too amorphous" for a precise definition and an elitist concept which should not be elevated to that of a fundamental right. Suhrith Parthasarathy, The Constitution, refreshed, The Hindu, 26 August, 2017

[226] Bench of three judges comprising Justices Chelameswar, Bobde, and C. Nagappan passed an order that a Bench of appropriate strength must examine the correctness of the decisions in M P Sharma v Satish Chandra, District Magistrate, Delhi, 1954 (Eight Judge Bench) and Kharak Singh v State of Uttar Pradesh, 1964 (Six Judge Bench). In particular it ordered that the Court must decide whether we have a fundamental right to privacy.

[227] Everything You Need to Know About the Aadhaar Case Before the SC Verdict, The Wire, 26 September 201

[228] Bill No. 47 of 2016, The Aadhaar (Target Delivery of Financial and Other Subsidies, Benefits and Services) Bill, Introduced In Lok Sabha, 11 March 2016

[229] A bill can be claimed to be money bill if it pertains to government spending and appropriations and consequently, does not require approval by both Houses.

[230] Foreword, Dissent on Aadhaar

[231] As Introduced In Lok Sabha, Bill No. 47 The Aadhaar (Target Delivery of Financial and Other Subsidies, Benefits and Services) Bill, 2016

[232] Section 139AA of the Income Tax Act

[233] The Central Board of Direct Taxation (CBDT) even refused to provide this information when a Right to Information (RTI) suit was filed, even though this information should have been in the public domain under Section 4(1)(c) of the RTI Act, 2005, as it constitutes facts relevant for formulating im- portant policies and decisions affecting the public.

[234] Kehar C.J., Agrawal J., Nazeer J., and himself

[235] Nariman J., Kaul J., Bobde J., Sapre J., and Chelameswar J.

[236] Para 447(4)(h) at page 560

[237] Vrinda Bhandar and Rahul Narayanan, In Striking Down Section 57, SC Has Curtailed the Function Creep and Financial Future of Aadhaar, The Wire

[238] Novopay was a digital payments startup incubated by Khosla Labs and being built by a number of ex-Aadhaar volunteers, including former technology Srikanth Nadhamuni, formerly Aadhaar's head of technology, and Sanjay Jain, formerly Aadhaar's chief product manager.

[239] India Brand Equity Foundation (IBEF), A Public Digital Infrastructure, India Adda-Perspectives on India, 27 January 2023

[240] ISpirt, India Stack takes the Digital India campaign to a whole new level. Dec 21, 2015.

[241] Ibid.

[242] India Stack

[243] N.S. Ramnath, Aadhaar: A quiet disruption, Founding Fuel, 2016 https://www.foundingfuel.com/article/aadhaar-a-quiet-disruption/

[244] Vivek Raghavan, Sanjay Jain, Pramod Varma, India Stack - Digital Infrastructure as Public Good, Communications of the ACM, November 2019, Vol. 62 No. 11, Pages 76-81

[245] Source: BIS Papers No 124, authors Siddharth Tiwari, Sharad Sharma, Siddharth Shetty and Frank Packer

[246] eSign

[247] Digilocker

[248] IRDAI advises companies to enable Digilocker for storage of policy papers, Medianama, Feb 16, 2021.

[249] Department of Electronics and Information Technology, Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016, 21st July, 2016

[250] The Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Amendment Rules, 2017

[251] Livemint, How the Indian state is building a new generation of digital public goods. October 14, 2016.

[252] Reserve Bank of India, Report of the Technical Committee on Mobile Banking, February 2014.

[253] Aparajita Choudhury, How 27-year-old Nikhil Kumar and team built the BHIM app in just 3 weeks, YourStory, 13 February, 2017.

[254] Ispirt, UPI – The Revolution in Payment Industry. August 13, 2016.

[255] The Economic Times, RS Software wins additional contracts from National Payments Corporation of India, February 24, 2016.

[256] Patent - An electronic payment system and method thereof, WO2017221085A1

[257] NPCI, Unified Payments Interface (UPI) Product Overview

[258] Ministry of Finance, Office Memorandum, Promotion of Payments through Cards and Digital Means, Department of Economic Affairs Currency & Coinage Division, 29 February, 2016

[259] Ministry of Finance, Office Memorandum, Promotion of Payments through Cards and Digital Means, Department of Economic Affairs Currency & Coinage Division, 11 March, 2016

[260] NPCI, Circular 01 - Enablement of UPI for thousand employees; NPCI, Circular 02 - Enablement of UPI for thousand employees.

[261] Reserve Bank of India, Payment and Settlement Systems in India: Vision-2018, 23 June, 2016

[262] Ministry of Finance, Committee on Digital Payments headed by Shri. Ratan P Watal, Principal Advisor, NITI Aayog and former Finance Secretary submits its Final Report to the Union Finance Minister Shri Arun Jaitley today, Press Information Bureau, 9 December, 2016

[263] Nikhil Kumar: BHIM's Star, Now Building Fintech Bridges - Forbes India. Forbes India, February 12, 2020.

[264] Medianama, Razorpay will have revenue sharing deals with banks for UPI payments, September 23, 2016.

[265] Live Mint, Demonetization 3rd anniversary: How digital payments picked up post note ban, November 8, 2019.

[266] Money Control, Govt to incentivise UPI and RuPay transactions. Banks, UPI players see revenue hopes, December 16, 2021.

[267] Ministry of Finance, Committee on Digital Payments, Report Medium Term Recommendations To Strengthen Digital Payments Ecosystem, December 2016

[268] Official Twitter Handle Prime Minister of India Incentives to encourage digital payments, 9 December, 2016

[269] NITI Aayog, NITI Aayog announces launch of the schemes - Lucky Grahak Yojana and Digi-Dhan Vyapar Yojana - for incentivising digital payment, Press Information Bureau, 15 December, 2016

[270] Financial Express, Fintech firms hit: Rising UPI payments eat into banks' and fintech firms' incomes, April 4, 2022.

[271] ICRA, National Payments Corporation of India (NPCI): Rating reaffirmed, 20 September, 2022

[272] Reserve Bank of India, Discussion Paper on Charges in Payment Systems. 17 August, 2022

[273] Ibid

[274] Reserve Bank of India, 'Special measures upto March 31, 2017: Rationalisation of Merchant Discount Rate (MDR) for transactions upto ₹ 2000/-', 16 December, 2016

[274]Reserve Bank of India, Rationalisation of Merchant Discount Rate (MDR) for Debit Card Transactions – Continuance of Special Measures, 30 March, 2017

[275] Kelkar, N. Top retailers flag RBI's revised MDR charges, The Week, 11 December, 2017

[276] Ministry of Electronics and Information Technology, Notification Subsidizing MDR charges on Deblt Cards/BHIM UPIAGPS trensrctions of value lcss than or equal to Rs. 2000, 27 December, 2017

[277] Reserve Bank of India, Committee on Deepening of Digital Payments, 8 January, 2019

[278] Reserve Bank of India, Payment and Settlement Systems in India: Vision – 2019-2021, 15 May, 2019

[279] Rule 119AA to the Income Tax Rules, 1962 notified by the Central Board of Direct Taxes

[280] Pandey, S. Payment firms, banks seek Rs 8,000-cr Budget support. The Financial Express. 10 January, 2023

[281] Reserve Bank of India, 13th Meeting of the FSDC Sub Committee – New Delhi, 09 August, 2014

[282] Reserve Bank of India, Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by NBFCs, 2015

[283] Reserve Bank of India, RBI Central Board meets at Chennai: RBI to allow Account Aggregator NBFCs; to set up Financial Inclusion Advisory Committee, 2 July, 2015

[284] Reserve Bank of India, RBI floats Draft Regulatory Framework for Account Aggregator Companies to facilitate Consolidated Viewing of Financial Assets Holdings, 03 March, 2016

[285] Reserve Bank of India, Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016

[286] Reserve Bank of India, Master Direction- Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016

[287] DigFin, What is the India Stack? Nandan Nilekani explains, 28 July 2020

[288] Srikanth Lakshmanan, Exclusive: RBI Issues In-Principle Licences To 5 Account Aggregators, Medianama, 19 November, 2018

[289] A private insolvency information utility jointly held by banks and regulated by Insolvency and Bankruptcy Board of India (IBBI)

[290] Sahamiti, Mr Nandan Nilekani Introducing Account Aggregator, 11 August, 2019

[291] Reserve Bank of India, Report of the High-Level Committee on Deepening Digital Payments, May, 2019

[292] Ibid.

[293] Sahamati was incorporated as a not-for-profit private limited company under Section 8 of the new Companies Act of India.

[294] Sahamiti

[295] Reserve Bank of India, Technical Specifications for all participants of the Account Aggregator (AA) ecosystem, 08 November, 2019

[296] Supranote 135 Indian Ministry of Science and Technology, 2012

[297] Ibid

[298] Reserve Bank of India, Electronic Consent Framework, Technology Specifications, Version 1.1

[299] Ibid

[300] As introduced in the Lok Sabha Bill No. 373 of 2019, The Personal Data Protection Bill, 11 December, 2019

[301] Builds on the National Health Stack Strategy Paper, published by NITI Aayog in July 2018

[302] National Health Authority, Ayushman Bharat Digital Mission - Creating India's Digital Health Ecosystem

[303] Lok Sabha, Report of the Joint Committee on the Personal Data Protection Bill, 2019, 21 December, 2021

[304] iSPIRT, Announcing Data Empowerment And Protection Architecture (DEPA) Workshop On 18th May, 5 May 2019

[305] State Bank of India, IDFC First, HDFC Bank, ICICI Bank, IndusInd Bank, Axis Bank, DICE India, and Kotak Bank amongst others; CredAll represents HDFC, ICICI Bank, Axis Bank, SBI, and IDFC First Bank, among others; The four major financial sector regulators: Reserve Bank of India (RBI), Securities & Exchanges Board of India (SEBI), Provident Fund Regulatory & Development Agency (PFRDA), Insurance Regulatory and Development Agency India (IRDAI), and the Telecom Regulatory Authority of India. The Ministry of Finance (including the Department of Revenue, the Department of Economic Affairs, the Department of Financial Services, and the Financial Sector Development Committee), the Ministry of Health and Family Welfare, the National Health Authority, and the Ministry of Information Technology (MeitY).

[306] Srikrishna headed the parliamentary committee which drafted the 2019 PDP Bill; Bhattacharya is former chairperson of the State Bank of India who joined the board of directors of Reliance Industries shortly after her retirement; Mathan is partner at the Trilegal law firm.

[307] To build a specification for a consent artefact based on the one introduced by MeitY:

[308] For e.g. in the financial sector, the Financial Information Standard lays down the required shared elements of a bank statement across institutions.

[309] Reserve Bank of India. Section 6(6), Master Direction- Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016.

[310] FIPs are institutions like banks or insurance providers that hold user data while FIUs are entities like lending agencies (including banks) that receive consumer financial information through AAs and use it to provide services such as wealth management, insurance, or loans.

[311] NITI Aayog.Data Empowerment and Protection Architecture: Draft for Discussion. 2020

[312] On 3 January 2020 Finvu owned by Cookiejar Technologies Private Limited, NESL Asset Data Limited and CAMSFinServ were granted NBFC-AA operating licenses by RBI.

[313] First-ever AA hackathon organized, 50 teams, 500 developers, 1 month in July 2020. In September, 2020 v1.1.2 Technical Standards published by ReBIT. Sahamati launched the Central Registry v1.0 in March 2020 and a Certification Framework v1.0 in September 2020. The first 10 institutions (including 3 AAs) achieved certification by December 2020,

[314] Reserve Bank of India, Technical Specifications for all participants of the Account Aggregator (AA) ecosystem, 08 November, 2019

[315] The four AAs: OneMoney, Finvu CAMS Finserv, and NADL The banks: State Bank of India, ICICI Bank, Axis Bank, IDFC First Bank, Kotak Mahindra Bank, HDFC Bank, IndusInd Bank, and Federal Bank

[316] Major Indian banks join Account Aggregator network to help individuals conveniently access and digitally share their financial data, 2 September, 2021

[317] Thimmaya Poojary, Eight banks join account aggregator network, a newly launched open digital financial platform, YourStory, 02 September, 2021,

[318] UIDAI Committee on Biometrics, Biometrics Design Standards For UID Applications, December 2009

[319] UIDAI, 'Role of Biometric Technology in Aadhaar Enrollment', 2012

[320] The pilot of the UID project sampled data from just 20,000 people. On the false positive identification rate, i.e. the probability of mistaken identity, the UIDAI said it will look at the point where the rate is 25,000 false positives for every I billion comparisons. Moneylife, How UIDAI goofed up pilot test results to press forward with UID scheme, 18 March 2011.

[321] Is Your Aadhar Biometrics Safe? Firms Accused Of Storing Biometrics And Using Them Illegally, The Outlook,

[322] Carnegie Endowment, Digital Public Infrastructure: The Key to 21st Century Innovation and Growth, 13 April 2023

[323] Ibid

[324] Filed by Bengaluru-based Col Matthew Thomas, a petitioners against Aadhaar

[325] Logs include the Aadhaar number, auth request, CIDR's response, information disclosed upon authentication, and the person's consent for authentication

[326] T Prashanth Reddy, Did SC Re-Affirm that Aadhaar Database Could Be Used for Criminal Investigations?, The Wire, 16 October 2018

[327] Criminals are able to use the credentials, silicon fingerprints, printouts of the IRIS scan and the configured laptops of authorised agents, to gain access to the system or create fake identities.

[328] 'Question Of National Security,' Nearly 100 Aadhaar-Related FIRs Brought To UIDAI's Notice: Report, ABPLive, 6 June 2022

[329] Ajay Sura, UIDAI must share data for heinous crime probe: HC, The Times of India, 19 April 2023

[330] Daily Pioneer, First FIR filed under Aadhaar Act after two found having same biometric info, March 28, 2017.

[331] Report of the Comptroller and Auditor General of India on Performance Audit of the Functioning of Unique Identification Authority of India, Report No. 24 of 2021

[332] The Wire, A Pakistani Spy and Lord Hanuman Walk Into an Aadhaar Centre. What Does the UIDAI Do?, January 15, 2018.

[333] Over 1000 Aadhaar cards found dumped on Tamil Nadu river bank, 2016

[334] Raju, Raja Siddharth, Sukhdev Singh, and Kiran Khatter. "Aadhaar Card: Challenges and Impact on Digital Transformation." *arXiv preprint arXiv:1708.05117* (2017).

[335] Rachna Khaira, Rs 500, 10 minutes, and you have access to billion Aadhaar details, The Tribune, 3 January 2018

[336] Huffington Post, UIDAI's Aadhaar Software Hacked, ID Database Compromised, Experts Confirm, September 11, 2018.

[337] World Economic Forum, The Global Risks Report 2019

[338] Twitter User Highlights Security Flaws in UIDAI's mAdhaar App for Android Devices, User Data Could be Compromised, FirstPost, 24 January 2018

[339] Singh, S. New Aadhaar data leak exposes 11 crore Indian farmers' sensitive info. Zee News.14 June, 2022

[340] The Hindu BusinessLine, 1 bn records compromised in Aadhaar breach since January: Gemalto, 6 December, 2021

[341] Copying Thumb Impressions on Butter Paper, Using Aadhaar to Steal Money, UP Cybercriminal Gang Busted, DailyHunt, 7 May 2023

[342] Reuters, Critics of Aadhaar project say they have been harassed, put under surveillance, February 13, 2018

[343] CAG Audit report number 24 of 2021. (Paragraph 3.5.1)

[344] Bhatia, Amiya, and Jacqueline Bhabha. "India's Aadhaar scheme and the promise of inclusive social protection." *Oxford Development Studies* 45, no. 1 (2017): 64-79.

[345] UIDAI asks banks to use Aadhaar eKYC for DBT users; voluntary offline Aadhaar for other customers, The Economic Times, 28 October 2018

[346] Srinivas Kodali, How Private Sector Slowly Regained Access to Aadhaar Post SC Judgment, The Wire, 14 June 2019

[347] Ministry of Electronics and Information Technology, Aadhaar Authentication for Good Governance (Social Welfare, Innovation, Knowledge) Rules, 2020

[348] Aadhaar (Enrolment and Update) (Tenth Amendment) Regulations, 2022, November 2022

[349] SBI Research, Ecowrap Issue No. 42. The State Bank of India. 3 November 2022

[350] Pursuant to RBI powers under section 10 and section 18 of the PSS Act

[351] Reserve Bank of India, Guidelines on Regulation of Payment Aggregators and Payment Gateways, 17 March 2020 (Updated as on November 17, 2020)

[352] Master Directions on Prepaid Payment Instruments (PPIs)

[353] NPCI International Payments Limited NIPL

[354] Report of the Comptroller General of India, Annexure I List of Government companies/ Government controlled other companies which came under/ went out from the purview of CAG Audit during 2019-20,

[355] Department of Economic Affairs, Ratan P Wattal - Committee on Digital Payments, December 2016.

[356] Medianama, Razorpay will have revenue sharing deals with banks for UPI payments, September 23, 2016.

[357] Yourstory, Interoperability triggers a tussle between digital wallets and payments banks, August 13, 2018.

[358] Medianama, ICICI's blocking of PhonePe VPA's raises questions about governance of NPCI & UPI, January 16, 2017.

[359] Ibid

[360] 'Storage of Payment System Data' 6 April, 2018

[361] Panday J. and Lakshmanan S. Unpacking RBI's Quest to Have All Payment Data Stored Within India's National Boundaries, 27 October, 2018

[362] Singh, D. Law enforcement agencies favour data localisation, The Economic Times 18 October, 2018

[363] Mastercard shifts focus to Southeast Asia, LatAm after India ban, Russia exit, Reuters, 26 May 2022

[364] Master Circular on Customer Service in Banks

[365] Frequently asked Questions

[366] In a Writ Petition/PIL filed by the Centre For Accountability And Systemic Change (CASA) in 2018, RBI filed an affidavit that clearly stated that WhatsApp was not 100 percent compliant with the data localisation mandate for payment services.

[367] Advait Palepu, A. WhatsApp Pay Roll-Out Delayed Due To Data Localisation Hurdles, NPCI Tells Supreme Court, Medianama, 3 February, 2021

[368] Mathi, S. Why Is NPCI Limiting WhatsApp's UPI Userbase? Medianama 14 April, 2022

[369] Bose, S. WhatsApp allowed to expand UPI user base to 100 million, says NPCI, The Financial Express, 13 April, 2022

[370] Application had been filed by CASA questioning the permissibility of the limited users mandate by NPCI to WhatsApp even as the RBI admitted the company to be non-compliant.

[371] Tarush Bhalla, T. NPCI starts auditing data localisation norms for digital payment firms, LiveMint, 12 May 2020

[372] Kailash Babar, Data centers to enable India's trillion-dollar digital economy growth; Mumbai, Chennai to lead, report, The Economic Times, 15 March 2020

[373] Finshots, Understanding Data Localisation Rules, 14 April, 2022

[374] National Informatics Centre, Digital Payments driving the growth of Digital Economy

[375] RazorPay. UPI AutoPay: A Powerful Addition to Your Payment Options Bouquet. 27 July 2020,

[376] Payal Ganguly, After its success in payments, fintech startup Juspay is all set to build credit infrastructure rails. YourStory, 8 January, 2022.

[377] Reserve Bank of India Statement on Developmental and Regulatory Policies. 16 June, 2022

[378] Supranote 91 (Mishra et al. 2023)

[379] Shayan Ghosh, S. and Gopakumar, G. How RBI fought and lost battle to charge for UPI transactions, LiveMint, 22 August 2022

[380] Soni, S. UPI: Peer-to-merchant transactions see 110% YoY growth in May 2023; value increased by 60% to Rs 3.44 lakh cr, The Financial Express, 4 June, 2023

[381] Bose, S. Fintech firms hit: Rising UPI payments eat into banks' and fintech firms' incomes.4 April, 2022

[382] Shashidhar. K.J., The weaponization of cashbacks on UPI by Google Pay. The Observer Research Foundation. 28 October, 2019

[383] Goenka, T. and Bose, S. WhatsApp UPI transactions slide after withdrawal of cashbacks, The Financial Express, 10 August, 2022

[384] s, Pratik Bhakta, P. and Shrivastava, A., Zero merchant fee is a force multiplier for digital payments: Paytm's Vijay Shekhar Sharma, The Economic Times, 10 July, 2019

[385] Verma, S. BHIM's 17.2M Transactions Accounted For Only 1.8% Of UPI Payments In September 2019, Medianama, 7 October, 2019

[386] Merchant, Z. Zero MDR On Merchants Will Lead To Collapse Of Payments Acquiring Industry, Says PCI, Medianama, 10 July, 2019

[387] For How Long Will the UPI Ecosystem Survive without MDR Charges? Moneylife, 7 October 2022

[388] Bankers Seek MDR On RuPay Debit Card Use: Report, The Outlook, 25 May 2023

[389] CashlessConsumer, MeitY response to RTI about MDR subsidy dispersal to banks. 29 March 2019

[390] CashlessConsumer, Meity response to RTI about the MDR subsidy spends for calendar year 2019, 7 January 2020

[391] MEITY Annual Report 2020-2021

[392] Singh, M. India to spend $320 million to promote homegrown payments network, TechCrunch, 11 January 2023

[393] Mathi, S For How Much Longer Will The Indian Government Bankroll UPI And RuPay? MediaNama, 23 January, 2023

[394] The Federal, Incentives on UPI 'appropriated by banks', says Payments Council chairman, 22 August, 2022

[395] Reserve Bank of India, Discussion Paper on Charges in Payment Systems. 17 August, 2022

[396] ENS Economic Bureau, Finance Ministry allays worries on UPI charges, says providers may seek 'other means' 22 August, 2022

[397] An interchange fee of 0.5 percent is applicable on fuel payments, 0.7 percent for the post office, telecom, utilities, agriculture and education, 0.9 percent for supermarket payments, and 1 percent for insurance, mutual fund, government and railways.

[398] Christopher, N. India's plan to export its wildly successful digital payments system, Rest of the World, 10 April, 2023

[399] Nair, V. NPCI Imposes Cap On Share Of UPI Transactions NPCI puts a 30% market share cap on transaction volumes for third party applications providing UPI services. BQ Prime. 6 November 2020

[400] Reserve Bank of India, Draft Framework for authorisation of a pan-India New Umbrella Entity (NUE) for Retail Payment Systems. August 2020

[401] Singh, M.India's central bank abandons UPI rival project, TechCrunch, 7 April, 2023

[402] Tata Group came together with Kotak Mahindra Bank, Airtel Digital, HDFC Bank, Flipkart, Mastercard and PayU. Amazon formed a grouping with ICICI Bank, Axis Bank, Visa, Pine Labs and BillDesk. Paytm partnered with the likes of Ola Financial, Policybazaar, and IndusInd Bank. consortium of Google, Facebook, and SoHum Bharat, along with Jio Infosystems.

[403] T. Rudra, RBI Puts NUE Licencing On Hold As Proposals By Consortiums Fall Short Of Expectations, Inc 42, 7 January 2023

[404] Shreyashi, T. New umbrella entities explained: Why India has delayed their retail payment systems. The Financial Express, 13 September 2021

[405] Press Information Bureau, PM addresses first meeting of Finance Ministers and Central Bank Governors under India's G20 Presidency, 24 February 2023

[406] Live Mint, RBI opens up UPI for feature phones, no Internet needed, March 9, 2022.

[407] Features and Benefits of UPI 2.0

[408] UPI Lite

[409] Ray, A., UPI to now allow borrowers to access digital credit lines from banks, The Economic Times, 6 April, 2023

[410] Kumra, G. Why Infosys's cofounder Nilekani is urging leaders to use tech for good, McKinsey 12 July, 2022

[411] Poddar, U. Are your UPI payments farming your personal data without your consent? 28 March, 2023

[412] Reserve Bank of India, Payments Vision 2025

[413] Bose, S. RBI working to expand use of UPI for cross-border remittances, The Financial Express, 31 March 2022; Sauradeep Bag, UPI in the Gulf: Revolutionizing remittances, Observer Research Foundation, 20 February, 2023

[414] Christian Perez, What Does Russia's Removal From SWIFT Mean For the Future of Global Commerce? Foreign Policy

[415] Greene R. How Sanctions on Russia Will Alter Global Payments Flows, Carnegie Endowment for International Peace

[416] Bloomberg,China's Fledgling Cross-Border Payments System Grows Its Reach,23 September, 2021

[417] Simon A. Payment Giant Has SWIFT Alternative for Indian Expats, Bloomberg. Saloni Shukla, NPCI takes UPI global, ties up with leading payments provider PPRO, The Economic Times, 17 November 2021

[418] Luthra P. Cybercrimes in India may rise if no action is taken: Jayant Sinha, CNBCTV18

[419] MoneyControl News, UPI scams on the rise: Know how to protect yourself while making payments via UPI, 31 May 2023

[420] Dhankhar, L. Nuh's hilltop 'call centres' emerge as epicentres of fraud, 30 June, 2023

[421] Mohan, C., Datta, S., Venkatanarayanan, A., & Rizvi, K. Tackling Retail Financial Cybercrimes in India, 2022

[422] Kalra, A. Exclusive: India found cybersecurity lapses at National Payments Corp in 2019 - government document, Reuters, 30 July 2020

[423] Reserve Bank of India, Oversight Framework for Financial Market Infrastructures and Retail Payment Systems, 13 June, 2020

[424] Principles for Financial Market Infrastructures (PFMI)

[425] NPCI - PFMI Disclosure Report

[426] Moneylife Digital Team, Security Audit Found 40 Vulnerabilities in NPCI including Several 'Critical' and 'High' Risk: Report, 30 July 2020

[427] Ibid Kalra A.

[428] Ramanathan A. The UPI frauds undermining India's payments fairytale, The Ken, 4 January 2022

[429] Ministry of Home Affairs, Details about Indian Cybercrime Coordination Centre (14C) scheme

[430] Account Aggregator Dashboard

[431] Supranote 91 (Mishra et al. 2023)

[432] Reserve Bank of India, Inclusion of Goods and Service Tax Network (GSTN) as a Financial Information Provider under Account Aggregator Framework, 23 November, 2022

[433] Supranote 91 (Mishra et al. 2023)

[434] Supranote 330 Saikat Datta

[435] FinMin permits 22 finance companies to undertake Aadhaar-based verification of clients, The Hindu, 5 May 2023

[436] India Brand Equity Foundation, A Public Digital Infrastructure: India Stack