Chapter 2: India's Push for Data Localization – Postcolonial Sovereignty in the Age of Digital Empires

I. Introduction: Reclaiming the Digital Territory

India's push for data localization is not merely a regulatory gesture—it is a signal flare from a postcolonial state asserting autonomy in a digital ecosystem historically dominated by Western and now increasingly Sino-American infrastructural powers. While the age of synthetic sovereignty is characterized by the erosion of traditional borders and the rise of algorithmic control, India's localization push represents a counter-hegemonic assertion of state power, aiming to reclaim digital territory and shape the rules of engagement with global platforms. As the second-most populous nation and the largest democracy, India's demand that global firms store and process Indian users' data within its borders reflects more than a desire for compliance—it signals a strategic reclamation of narrative control, economic leverage, and jurisdictional power.

Fueled by its status as the second-most populous nation and a rapidly expanding digital economy, India's localization demands not only assert political will but also wield significant economic leverage, potentially reshaping global data flows and market dynamics. With over 800 million internet users and the fastest-growing major digital economy, India's market represents a prize too valuable for global tech firms to abandon, creating asymmetric bargaining power that the Indian state has strategically deployed in its sovereignty project.

This is not just data governance—it's digital decolonization. In a world where attention is mined and sovereignty is increasingly synthetic, India's localization mandate reframes data infrastructure as contested geopolitical terrain.

II. Historical Context: From East India Company to Cloud Sovereignty

India's data localization agenda must be read through a historical lens. The subcontinent's experience of colonial exploitation through extractive information systems—led by entities like the East India Company—echoes eerily in the architectures of today's global platforms. British imperial rule relied heavily on "extractive information systems," such as meticulously detailed census data used for taxation and social control, and extensive mapping projects designed to facilitate resource extraction and administrative control. The colonial administration's systematic classification of populations by caste, religion, and ethnicity not only facilitated governance but also reified social divisions that continue to shape Indian society today.

The colonial practice of categorizing and classifying populations finds an unsettling echo in the algorithmic profiling of users by global platforms, where granular data points are used to predict behavior and target advertising, raising similar concerns about power imbalances and the potential for discrimination. Just as colonial administrators extracted information to consolidate control and maximize economic gain, modern platforms harvest behavioral data to generate profit while shaping social norms and political discourse.

The Personal Data Protection Bill (now evolved into the Digital Personal Data Protection Act, 2023) is thus framed not as technocratic policy, but as an attempt to invert digital colonialism. Data localization is thus envisioned as a "firewall" not just protecting data from external access

but also shielding India's cultural and political sovereignty from the homogenizing effects of global platform logic and the potential for external manipulation of its digital public sphere. By insisting that data physically reside within national borders, India attempts to reassert jurisdictional authority over the informational resources generated by its citizens—resources that have historically flowed outward to benefit foreign powers.

III. Platform Colonialism and the Corporate Cartography of Identity

Global platforms like Google, Meta, and Amazon have functioned as supranational actors within India—operating critical digital infrastructure, monetizing linguistic and cultural diversity, and curating behavioral identities via foreign-owned algorithms. Global platforms engage in a form of "corporate cartography of identity," meticulously mapping user behavior, preferences, and social connections to create detailed profiles that are then used to target advertising and shape content recommendations, effectively commodifying individual and collective identities. These data-driven maps become the basis for far-reaching decisions about content visibility, service access, and market opportunities.

In this "platform colonialism," linguistic diversity becomes a resource for targeted advertising, cultural practices are commodified through influencer marketing, and social connections are transformed into engagement metrics, all contributing to a system where Indian identity is fragmented and sold back to its citizens. Regional languages, once marginalized under British colonialism, face a different form of subordination as platforms measure their value primarily by market size and advertising potential rather than cultural significance or expressive richness.

India's insistence on localized storage disrupts this regime. It challenges the notion that cloudspace is neutral, asserting instead that data is territory—and whoever controls the data controls the narrative.

Google's autocomplete suggestion, "Is India a poor country?", exemplifies the dangers of algorithmic bias. It wasn't an objective truth but a distorted reflection of historical power imbalances and skewed data. India's localization push, in part, aims to create space for the cultivation of sovereign counter-narratives that challenge these algorithmic distortions. By reshaping the legal and technical infrastructure of data processing, India seeks not only control over information but also influence over how that information is contextualized, interpreted, and presented back to its citizens—a fundamental challenge to platform control over meaning-making.

IV. The Sovereignty Logic of Infrastructure

Data localization is also infrastructural nationalism. By requiring domestic data storage and processing, India is forcing the construction of local data centers, fueling a tech-industrial policy that converges with state-led development goals. India's data localization strategy can be seen as a form of "digital import substitution industrialization" (ISI), echoing postcolonial economic policies aimed at fostering domestic industry by restricting foreign competition. While this approach can stimulate local innovation and create jobs, it also carries the risk of inefficiency and higher costs. The mandate for local data centers has already triggered significant investments by global cloud providers, including Amazon Web Services, Google Cloud, and Microsoft Azure, all of which have established or expanded Indian data center operations.

This infrastructural sovereignty extends beyond physical data centers to encompass the digital architecture itself. Initiatives like India Stack and the Digital Public Infrastructure (DPI) framework aim to establish a sovereign digital ecosystem, providing interoperable platforms for identity verification, payments, and social service delivery. While these systems have the potential to empower citizens and improve access, they also raise concerns about data centralization and the potential for state surveillance. The Unified Payments Interface (UPI), a core component of India Stack, has revolutionized digital financial transactions by creating an open infrastructure that has significantly reduced dependency on global payment networks while simultaneously giving the state unprecedented visibility into financial behaviors.

India's ambitious plans—such as the India Stack and Digital Public Infrastructure (DPI) framework—exemplify a parallel sovereignty project: to create interoperable digital public goods that rival proprietary platforms and recenter the state as the arbiter of identity, authentication, and social delivery systems. By building alternative infrastructures, India aims not merely to regulate global platforms but potentially to supplant them with technologies more aligned with national priorities and values.

V. Democratic Contradictions: Between Autonomy and Surveillance

India's pursuit of digital autonomy is fraught with a tension that is not unique to the nation: the same infrastructure that empowers the state to resist external platform power can also be turned inward, enabling increased domestic surveillance and control over its citizens. This paradox reflects a global pattern where authoritarian and democratic regimes alike invoke sovereignty as justification for expanding state power over digital domains.

The Aadhaar biometric ID system, while intended to promote financial inclusion and efficient service delivery, has faced legal challenges due to concerns about privacy violations, data breaches, and its potential for mass surveillance, highlighting the inherent contradictions in a state-driven data localization agenda. Initially voluntary, Aadhaar has become nearly mandatory for accessing numerous government services and even many private sector offerings. With over 1.3 billion enrollments, it represents one of the world's largest biometric databases, creating unprecedented capabilities for state monitoring and control. The Supreme Court's landmark 2018 judgment upheld the constitutionality of Aadhaar while imposing limitations on its mandatory use, reflecting the ongoing tension between state power and individual rights.

Civil society organizations have raised alarms about the potential for data localization to facilitate surveillance capitalism by domestic firms or enable state repression. Reports of increased targeting of activists and journalists, internet shutdowns in regions like Kashmir, and the deployment of spyware against opposition figures all suggest that localization without robust privacy protections and independent oversight may simply replace foreign surveillance with domestic monitoring.

This raises a crucial question: Can data localization achieve genuine digital sovereignty, or does it merely shift the locus of control, replacing the external influence of global platforms with the internal authority of an increasingly powerful state? The answer may depend on the strength of democratic institutions and the robustness of checks and balances. Without strong privacy laws, independent regulatory bodies, and democratic oversight mechanisms, data localization risks

becoming a tool for consolidating state power rather than empowering citizens.

VI. Resistance and Geoeconomic Fallout

U.S. tech firms have actively resisted India's data localization mandates, engaging in intense lobbying efforts, threatening legal challenges through the WTO, and engaging in protracted negotiations with the Indian government to seek exemptions or softer interpretations of the regulations. The U.S. Trade Representative has explicitly criticized India's localization requirements as "trade barriers," while industry groups such as the U.S.-India Business Council have warned about potential economic costs and technical complexities.

Despite this resistance, India has largely maintained its course, though with some strategic compromises. The evolution from the more stringent 2019 draft bill to the 2023 Digital Personal Data Protection Act reflects some concessions to industry concerns, particularly regarding cross-border data flows for certain categories of information. These adjustments highlight India's pragmatic balancing act between asserting sovereignty and maintaining its position as a global digital services hub.

India's regulatory posture has inspired a growing movement of "data non-alignment," with countries like Brazil, Indonesia, and Nigeria echoing similar demands for greater control over their digital resources, forming a potential coalition of states seeking to resist the dominance of both Silicon Valley and Beijing and forge alternative models of digital governance. This emerging bloc shares concerns about digital colonialism, though they differ in their specific approaches to data governance. Brazil's General Data Protection Law (LGPD) and Indonesia's Government Regulation 71 reflect similar impulses toward digital sovereignty, creating a potential counterweight to both American platform capitalism and Chinese digital authoritarianism.

The geopolitical implications extend beyond bilateral U.S.-India relations. India's localization push occurs against the backdrop of increasing friction with China, including the banning of hundreds of Chinese apps such as TikTok and WeChat. This dual resistance to both American and Chinese digital influence positions India as a potential leader in defining a "third way" for digital governance—neither fully open nor completely closed, but selectively permeable based on national interests and values.

VII. Winners and Losers

Winners:
Indian state institutions (gain greater control and revenue, but risk overreach); domestic tech firms (benefit from increased market share, but face pressure to comply with state demands); postcolonial theorists and digital rights activists (see validation of their arguments, but face challenges in ensuring equitable outcomes). The data center industry has experienced particular growth, with capacity in India expected to double by 2025, creating new economic opportunities and technical expertise. Middle-class consumers may benefit from improved service quality as platforms optimize for local conditions, though potentially at higher costs.

Losers:
U.S.-based tech monopolies (lose market share and face increased compliance costs); the

global 'free flow of data' narrative (is challenged, but its benefits are also questioned); civil society (risks increased state surveillance, particularly activists and marginalized communities). Small businesses face potential disadvantages as compliance costs disproportionately impact smaller players who lack the resources to implement complex data management systems. Rural and economically disadvantaged populations may experience reduced access if global platforms decide to limit services in response to regulatory requirements.

The distribution of benefits within Indian society remains uneven. Urban, educated, and economically advantaged citizens may gain from improved digital services and expanded job opportunities in the domestic tech sector. However, marginalized communities—particularly those already subject to state surveillance or discrimination—face heightened vulnerabilities if localization strengthens surveillance capabilities without corresponding protections.

The greatest vulnerability lies with civil society organizations, journalists, and activists who challenge state power. For these groups, the potential for increased surveillance under localization mandates represents a significant threat, particularly as India has witnessed growing restrictions on civil liberties in recent years. The ultimate test of data localization will be whether it serves to enhance citizens' rights or merely consolidates state power over an increasingly digitized society.

VIII. Conclusion: The Data Border as a Postcolonial Fault Line

India's data localization strategy draws a "data border" that reflects a postcolonial fault line in the digital age. It is a necessary act of self-determination, but its ultimate success will be judged not by its ability to exclude external powers, but by its capacity to foster a just and equitable digital society within its own borders—a society where digital rights are as fiercely protected as digital territory. This border is not merely technical or legal but represents a philosophical claim about the relationship between citizens, their data, and the state in a postcolonial context.

The ambiguity of sovereignty in the digital age remains pronounced. While traditional sovereignty centered on territorial control and monopoly of force, digital sovereignty encompasses control over information flows, algorithmic decision-making, and the architecture of attention itself. India's attempt to reassert state authority over these domains challenges the deterritorialized power of global platforms, but also raises questions about the nature and limits of state power in the digital realm.

India's data localization strategy should not be seen as mere protectionism. It is an act of digital nation-building, aimed at redrawing the borders of sovereignty in a post-network age. Where TikTok exposed the vulnerabilities of cognitive borders, India builds firewalls of jurisdictional muscle. But sovereignty, synthetic or otherwise, remains ambiguous. The data wall may keep the empire out—but it can also become a mirror, reflecting the shape of a state's internal authoritarian desires. The future of sovereignty lies in whether these borders protect freedom—or simply reassign control.

In this sense, India's data localization experiment represents one of the most significant tests of whether postcolonial nations can chart an independent course in the digital age—one that reclaims autonomy from both Western and Eastern digital hegemons while fostering democratic values and individual rights. The outcome of this experiment will have profound implications not

only for India but for the global architecture of digital governance in the coming decades.