Digital Governance Assemblages: Reconfiguring Territory, Authority, and Rights in Comparative Perspective

Ge Xin *

Abstract

This article examines key problems and paradoxes of contemporary digital governance by moving beyond static, dichotomous models. It introduces and applies assemblage theory as a novel analytical framework to interpret digital governance not as a set of fixed regimes, but as dynamic, contingent, and contested socio-technical formations. Through a comparative analysis of three distinct governance assemblages—India's Aadhaar (the Biometric State Assemblage), Brazil's Marco Civil da Internet (the Multi-Stakeholder Rights Assemblage), and Australia's eSafety Commissioner (the Co-Regulatory Safety Assemblage), this paper demonstrates how heterogeneous elements of technology, law, discourse, and actors combine to produce unique governance realities. The analysis identifies recurring paradoxes, most notably the tension between the deterritorializing properties of digital technologies and persistent state efforts to reassert territorial control. The study concludes that understanding these emergent assemblages is vital for developing adaptive, legitimate governance frameworks, offering specific operational strategies for public administrators to navigate the frictional inclusion, normative fragility, and sovereign overreach that define the current digital age.

Keywords: Digital Governance, Assemblage Theory, State Authority, Administrative Capacity

* School of Public Administration and Policy, Shanghai University of Finance and Economics, China
Email: xin.ge@mail.sufe.edu.cn
Received: August 8, 2025 Revised: December 19, 2025 Accepted: December 30, 2025

Introduction

The digital transformation of the twenty-first century is marked by a persistent paradox: technologies that promise unprecedented efficiency, connectivity, and empowerment are simultaneously potent instruments of control, fragmentation, and exclusion. From artificial intelligence mediating access to public services to global data flows that underpin modern commerce, digital infrastructures are no longer peripheral tools but the foundational architecture of contemporary society (Floridi, 2014; Hanisch et al., 2023). This dual-edged nature presents an acute challenge for governance: *how to harness the immense potential of digitalization for societal good while mitigating the complex risks it engenders.*

The global response to this challenge has yet produced a coherent, unified order. Instead, the landscape is characterized by "regime complexity" (Drezner, 2009; Alter, 2022; Xin et al., 2023; Meng et al, 2024)—a dense, messy, and nonhierarchical array of overlapping institutions, rules, and norms governing the digital sphere. Prevailing analyses often attempt to simplify this complexity by categorizing national approaches into static, dichotomous models, such as the "state-centric" versus the "market-driven" or "rights-based" paradigms (Baer and Gerlak, 2015; Fratini et al., 2024; Xin and Huang, 2025). While such typologies offer initial clarity, they are ultimately insufficient. They fail to capture the dynamic, co-constitutive relationship between technology and governance, where legal frameworks, technical architectures, and social practices continuously shape and reshape one another. The fragmentation observed is not merely a failure of coordination; it reflects a deeper contestation between competing projects to define the very nature of digital reality. States, firms, and civil society actors are not merely vying to set the rules of a common game; they are using technology and law to construct fundamentally different operational realities with distinct objectives, players, and playing fields.

This study develops new insights by examining well-documented cases through the lens of assemblage theory. Drawing upon the philosophical work of Deleuze and Guattari (1980) and the applied social theory of DeLanda (2006) and Sassen (2008), assemblage theory provides a framework for analyzing digital governance not as a set of fixed structures, but as a collection of dynamic, historically contingent, and constantly evolving socio-technical formations. In doing so, it moves beyond descriptive case narratives and uncovers deeper commonalities – notably, three underlying paradoxes of digital governance – that have not been well theorized in the Public Administration literature. While the empirical facts of India's Aadhaar, Brazil's Marco Civil, and Australia's eSafety framework have been reported elsewhere, our assemblage-based analysis integrates these facts in a

novel way, revealing emergent patterns and governance challenges that static models overlook. This represents a conceptual contribution: we offer a fresh theoretical framework and vocabulary for analyzing digital governance, which can guide both scholars and practitioners in understanding complex socio-technical systems.

This study explicitly addresses the following research questions: How do digital governance assemblages configure heterogeneous elements—technology, law, actors, and discourses—into distinct regimes, and what fundamental paradoxes arise from these formations? By dissecting the composition and dynamics of three cases from Global South and North, this paper illuminates the core paradoxes of digital governance – how the deterritorializing force of technology clashes with the persistent territorial ambitions of states, how normative ideals are contested by material power, and how seemingly neutral technical architectures become charged sites of political struggle.

The paper proceeds as follows: Part 2 operationalizes assemblage theory for the study of digital governance, tracing its intellectual lineage and elaborating the interconnected key concepts. Part 3 outline the methodology underpinning the selection and analysis of the cases. Part 4 applies this framework to the detailed analysis of the Indian, Brazilian, and Australian cases. Part 5 synthesizes these findings through a comparative discussion, before concluding with the implications for navigating current and future digital order.

Theoretical Framework: Assemblage in Digital Governance

To move beyond static descriptions of digital governance, an analytical toolkit capable of capturing inherent dynamism, heterogeneity, and contingency is required. Assemblage theory, as articulated in the works of Deleuze and Guattari (1980) and operationalized for social analysis by DeLanda (2006, 2016) and Sassen (2008), provides such a framework. This section will outline the core concepts of assemblage theory and adapt them to create a robust framework for deconstructing the complex realities of digital governance.

At its heart, an assemblage (a translation of the French *agencement*) is a multiplicity composed of heterogeneous parts that establishes functional relationships between them. It is not a pre-determined structure, but a contingent and historical construction; it is a process of fitting together, not a finished product (Phillips, 2006; Legg, 2011). A digital governance assemblage, therefore, is the specific, functioning configuration of diverse elements that come together to regulate a particular aspect of the digital sphere. These elements include technical artifacts (code, algorithms, server

architecture, fiber-optic cables, biometric scanners), legal instruments (laws, regulations, court rulings), institutional bodies (regulators, ministries, standards organizations), corporate actors (platforms, data brokers), user practices (circumvention, compliance, protest), and public discourses (narratives of "safety," "sovereignty," "freedom", etc.).

Unlike a holistic totality, where the parts are defined by their relationship to the whole, an assemblage is characterized by relations of exteriority (Marcus & Saka, 2006). This means that a component is autonomous and can be "unplugged" from one assemblage and "plugged" into another, and that the assemblage itself can change and evolve over time as its components are reconfigured (Legg, 2011). Assemblages emerge through specific historical trajectories, moments of crisis, and struggles over meaning and authority, rather than through linear institutional design (DeLanda, 2006; Savage, 2020). This perspective is particularly useful for digital governance, where regulatory frameworks often crystallize in response to technological disruptions, security incidents, or public controversies rather than deliberate constitutional planning (Katzenbach & Ulbricht, 2019).

In DeLanda (2006, 2016)'s works, he identified two key axes along which assemblages can be characterized. As illustrated in Figure 1, the first is the material-expressive axis. The material pole refers to the physical components of the assemblage—the bodies, technologies, and resources that give it substance, while the expressive pole refers to its symbolic and normative dimensions—the languages, ideologies, and cultural forms that give it meaning. The second is the territorializing-deterritorializing axis. A territorializing process is one that consolidates authority or boundaries, while a deterritorializing process is one that disrupts or transcends established boundaries. In our coding of cases, these definitions guided how we identified and categorized each element of the governance assemblage.

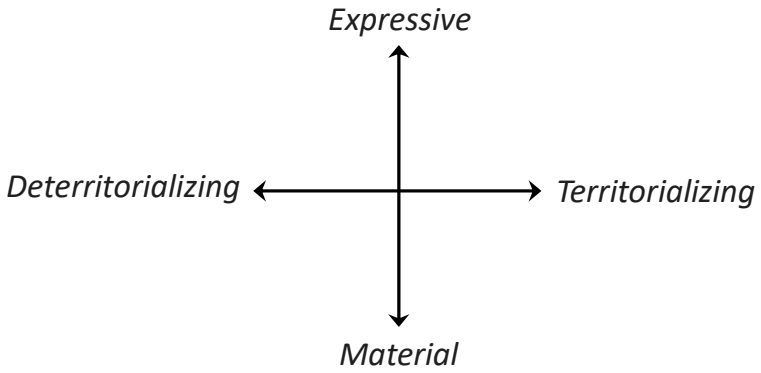

Figure 1. The Two Axes of Assemblage Theoretical Framework

Figure 1 above maps the two primary axes of assemblage theory. Along one axis, elements range from material components (e.g., infrastructure, technologies) to expressive components (e.g., narratives, legal norms). Along the other axis, forces range from territorializing (those that reinforce boundaries or control) to deterritorializing (those that disrupt or transcend established boundaries). This schematic diagram illustrates how any given governance assemblage can be analyzed: for instance, a particular law may be seen as an expressive component that has a territorializing effect, whereas a global platform is a material component that often exerts a deterritorializing influence.

Assemblage theory shares a family resemblance with actor–network theory (ANT) and other socio-technical approaches, but there are key differences. Unlike ANT, which "flattens" agency by treating human and non-human actors symmetrically, assemblage theory allows for emergent structures and acknowledges that components can be reconfigured without losing their identity (Müller, 2015; Bridge, 2021). This means our analysis recognizes, for instance, that a legal institution and a technical artifact interact, yet each can enter or exit the assemblage independently—an idea rooted in Deleuze's concept of relations of exteriority. This distinction is crucial for understanding how digital governance regimes can persist even as their technical components change, or conversely, how new technologies can destabilize existing legal orders.

Assemblage theory also extends and deepens existing work on regime complexity in global governance. While regime complexity scholarship emphasizes the coexistence of overlapping, partially coordinated institutions and rules across issue areas (Drezner, 2009; Alter, 2022), it largely treats governance as an interaction among formal regimes and organizations. Assemblage theory shifts the analytical focus from institutional overlap to the socio-technical ordering through which authority is enacted in practice. It highlights how governance outcomes are produced not only through formal rules but through the alignment of legal mandates, technological infrastructures, organizational routines, and discursive justifications (DeLanda, 2006; Sassen, 2008).

In the context of digital governance, this distinction is consequential. Digital power frequently operates through infrastructures, standards, and platforms that lie outside traditional regime boundaries yet exert binding effects on users and states alike (Plantin et al., 2018; Kornberger et al., 2017). Assemblage theory therefore allows us to explain why similar regulatory commitments—such as privacy protection or online safety—produce divergent outcomes across countries. Rather than asking whether regimes overlap or conflict, the assemblage perspective asks how heterogeneous elements are stabilized, contested, and reconfigured over time, offering a more fine-grained account of authority, legitimacy, and failure in digital governance.

Methodology

This study employs a comparative case design following Yin (2018)'s approach, aiming for analytic generalization. The three cases (India, Brazil, Australia) were purposefully chosen to maximize variation in context and governance models. This most-different systems strategy allows us to assess whether similar assemblage dynamics and paradoxes emerge across otherwise disparate settings. Our goal is theory-building: by examining extreme diversity, we generate insights that can inform broader public administration theory, rather than claiming statistical generalizability.

The selection is justified on three key grounds. First, the cases represent significant geographic and economic diversity. India and Brazil, as major Global South economies, offer insights into digital governance within contexts of developmental challenges and democratic traditions, while Australia provides a Global North perspective with advanced digital infrastructure. This spectrum allows for analysis of how divergent political cultures, resource constraints shape governance outcomes. Second, the cases cover distinct thematic areas of digital governance. India's Aadhaar exemplifies digital identity; Brazil's Marco Civil represents internet rights and infrastructure; Australia's eSafety Commissioner represents content moderation and safety. Third, the cases highlight contrasting governance models, ranging from state-led technocratic model of India, multi-stakeholder participatory model of Brazil and co-regulatory safety model of Australia.

Our analysis draws on multiple secondary sources, including legislative texts, policy documents, scholarly analyses, reputable media accounts, etc. We followed a systematic search and inclusion strategy to ensure coverage and credibility of evidence. Furthermore, we used diverse types of documents to cross-verify facts and interpretations, enhancing validity despite the lack of new field data.

As for data collection, we systematically gathered documents for each case. For India's Aadhaar, for instance, we collected laws (Aadhaar Act and regulations), government white papers, Supreme Court case transcripts, audit reports (CAG), academic studies (2010–2023), and major media investigations. Similar breadth was sought for Brazil and Australia. Searches were conducted via Google Scholar, official government websites, and news databases using keywords and combinations. We included sources that were either peer-reviewed, official (government or international organization reports), or well-documented journalism.

We operationalized assemblage theory by systematically coding each case's data along predefined dimensions. First, relevant documents were qualitatively coded for instances of material components (e.g. technical artifacts, infrastructure) and expressive components (e.g. legal principles, narratives). Second, we coded for territorializing processes (actions consolidating or enforcing boundaries/authority) versus deterritorializing processes (forces undermining or transcending those boundaries). This coding schema was derived from assemblage theory's core axes shown above. For example, in the Aadhaar case, we coded the biometric ID database as a material component and the discourse of "welfare inclusion" as an expressive component; making enrollment mandatory was a territorializing process, while authentication failures were a deterritorializing process. We repeated this for each case, then compared the coded assemblage maps to see common patterns and differences.

Case Analysis

Applying the assemblage lens outlined, we examine each case to deconstruct its material and expressive composition and the interplay of territorializing and deterritorializing forces.

The Biometric State Assemblage: India's Aadhaar

The Aadhaar program, India's Unique Identication system, represents a massive "Biometric State Assemblage" designed to re-terrirorialize state authority by translating the population's fluid identities into a centralized, machine-readable format. (Borah & Bhuyan, 2024).

The *material core* of this assemblage is the Central Identities Data Repository (CIDR), a centralized database storing the biometric (iris scans, fingerprints, facial photos) and demographic data of over 1.3 billion residents. This repository is supported by a nationwide network of physical enrollment centers where individuals' biometrics are captured using specialized hardware. The 12-digit unique Aadhaar number itself acts as a crucial material artifact, serving as a unique identifier that links an individual to their data. The entire system is supported by a physical infrastructure of enrollment centers and a digital layer of Application Programming Interfaces (APIs), the "India Stack", which allows various government agencies and private entities to "plug in" to the database for identity verification (Masiero and Shakthi, 2020).

The *expressive components* providing legitimacy are the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and the dominant state discourse of social inclusion and anti-corruption. The narrative posits that digital ID eliminates "ghost beneficiaries" and "leakages" in the welfare system, thereby serving the poor. Conversely, a counter-narrative from

civil society frames Aadhaar as a "surveillance tool" and a "panopticon," emphasizing the loss of privacy and the commodification of data (Khera, 2017). This discourse is, however, fiercely contested by a powerful counter-narrative from activists, academics, and civil society groups, who frame Aadhaar as an instrument of mass surveillance, a profound threat to individual privacy, and the foundation of an oppressive "surveillance state" (Masiero & Shakthi, 2020). The centralized nature of the database and its potential for cross-linking with other personal data streams were argued to create an unprecedented capacity for state control and monitoring (Singh, 2021).

The state engaged in intense *territorialization* by making the Aadhaar number the mandatory "key" to access the Indian state. Through seeding process, the unique number was linked to bank accounts, mobile SIM cards (via the Prevention of Money-Laundering Rules), tax filings (PAN cards), and the Public Distribution System (PDS) for food rations. This effectively eliminated the ability of individuals to exist in different administrative spheres with different identities; the assemblage collapsed the citizen's diverse interactions into a single, trackable data point. (Khera, 2017). The creation of the Unique Identification Authority of India (UIDAI), a powerful statutory body with centralized control over the identity ecosystem, further cemented the state's authority. By forcing individuals to disconnect their identities from traditional social assemblages—such as family, community, and paper records—and re-territorialize them onto the abstract plane of biometric data, the state sought to create a well governable population (Banerjee, 2016).

Despite the state's ambition to create a "frictionless" system, material constraints produced significant *deterritorializing* effects. The most critical has been biometric failure. Technological failures were pervasive. Authentication errors due to worn fingerprints (a common issue for manual laborers), poor connectivity in rural areas, or faulty equipment have frequently resulted in the denial of essential food rations, pensions, and other welfare benefits to millions of people (Khera, 2017). A Public Accounts Committee report noted biometric authentication failure rates as high as 12% in some rural districts, causing vulnerable citizens to miss out on rations. The UIDAI's own data from 2018 indicated an 88% success rate for government services, implying a significant failure margin. The "frictionless" design created "frictional exclusion".

Furthermore, the centralized database proved vulnerable to data breaches, a deterritorializing force that scatters the "territory" of identity beyond state control. Reports surfaced of demographic data being accessible via simple Google searches due to insecure government websites, and allegations of data sales on WhatsApp challenged the "secure vault" narrative (Jain, 2019). These failures contributed to sustained legal challenges, culminating in the 2017 Supreme Court judgment in K.S.

Puttaswamy v. Union of India that affirmed privacy as a fundamental right. The subsequent 2018 verdict struck down the mandatory linking of Aadhaar to private services like bank accounts and mobile phones (Section 57 of the Act). This resistance from the judiciary, coupled with grassroots activism and civil society critique, has worked to deterritorialize the state's absolute control, creating cracks and fissures in the biometric assemblage (Singh, 2021).

The Aadhaar assemblage demonstrates that biometric governance does not merely streamline welfare administration but fundamentally reshapes the relationship between citizen and state. By re-territorializing identity through centralized biometric infrastructure, the Indian state acquired unprecedented administrative visibility and coordination capacity. Yet this visibility is uneven and fragile. Evidence from audit reports, court judgments, and field studies shows that when biometric authentication fails—due to labor-worn fingerprints, infrastructural gaps, or data errors—the consequences are not administrative inconvenience but material deprivation. Aadhaar thus reveals a structural contradiction: a system optimized for efficiency at scale becomes brittle at the margins, where citizens most depend on welfare support. The promise of inclusion is therefore inseparable from new, technologically mediated forms of exclusion.

The Multi-Stakeholder Rights Assemblage: Brazil's Marco Civil da Internet

Brazil's Marco Civil da Internet (Law 12.965/2014), or Civil Rights Framework for the Internet, stands as an exemplar of the multi-stakeholder rights assemblage. Unlike India's state-centric model, this assemblage was constructed through a participatory process involving the government, civil society, and the private sector, aiming to territorialize Brazil's digital space around norms of free expression, privacy, and net neutrality (Hoskins, 2018). However, the history of the Marco Civil since its passage reveals the inherent fragility of a governance assemblage built primarily on normative consensus when confronted with entrenched material and institutional power.

The *material components* include the internet infrastructure (ISPs, fiber backbones) and the online platforms used for the legislative consultation process itself (e.g., the Cultura Digital portal), which materially enabled the multi-stakeholder participation (Hoskins, 2018). This digital infrastructure was not just a tool but a core component that enabled the law's multi-stakeholder nature. The assemblage also, of course, seeks to govern the physical internet infrastructure within Brazil's borders, from ISPs to data centers.

The *expressive components* are paramount here. The law is often termed the "Constitution of the Internet." Its core principles —net neutrality (Article 9), freedom of expression, and privacy

(Article 7)—form the normative "code" of the assemblage. The discourse frames the Internet as "essential to the exercise of citizenship," positioning the user as a citizen with rights rather than merely a consumer (Rodriguez & Pinho, 2015).

The passage of Law 12.965 was a *territorializing* act to stabilize the digital environment against arbitrary state, partisan or corporate interference (Steibel, 2012). It established clear boundaries. For net neutrality, Article 9 mandates that those responsible for transmission must treat data packets isonomically, without distinction by content, origin, or service. This was reinforced by Decree 8.771/2016, which clarified exceptions only for emergency services and technical requirements. For intermediary liability, Article 19 established a judicial notice-and-takedown regime, meaning platforms are only liable for third-party content if they fail to comply with a specific court order. This safe harbor was designed to prevent private censorship and stabilize the conditions for free expression.

While the legal text terrirorialized rights, economic and technical forces worked to *deterritorialize* them. The primary mechanism of this disruption is zero-rating. Despite the Marco Civil's net neutrality mandate, telecom operators (e.g., Claro, TIM) aggressively rolled out "zero-rated" plans where access to WhatsApp, Facebook, and Twitter does not count against data caps. Reports indicate that for millions of low-income Brazilians, these zero-rated apps are the internet, creating a "walled garden" (Freedom House, 2021). This practice deterritorializes the "open internet" envisioned by the law. While technically argued as compliant (users aren't charged), it materially discriminates against non-zero-rated traffic, effectively creating a two-tiered internet. The Comitê Gestor da Internet (CGI.br) and antitrust bodies (CADE) have struggled to consistently enforce the prohibition against these business models, revealing the "Normative Fragility" of the assemblage (Sautchuk-Patrício, 2022).

Furthermore, the assemblage faces deterritorialization from the judiciary itself. Frequent court orders to block WhatsApp (due to encryption preventing data handover in criminal cases) clash with the law's connectivity goals. Additionally, the Constitutional prohibition on anonymity is often weaponized to unmask users, undermining the privacy protections the Marco Civil sought to enshrine.

In brief, the Marco Civil illustrates the limits of rights-based digital constitutionalism when normative commitments are insufficiently anchored in enforcement capacity. While Brazil successfully territorialized a vision of the internet grounded in citizenship and fundamental rights, this normative territory remains vulnerable to economic power and judicial reinterpretation. Persistent zero-rating practices and court-ordered platform shutdowns demonstrate how material infrastructures and institutional authority can erode legal ideals without formally overturning them. The Brazilian case

shows that participatory lawmaking, while critical for legitimacy, does not by itself secure durable governance outcomes unless supported by sustained regulatory alignment and institutional capacity.

The Co-Regulatory Safety Assemblage: Australia's eSafety Commissioner

Australia's approach to digital governance represents another distinct model. The establishment of the eSafety Commissioner has given rise to a unique Co-Regulatory Safety Assemblage. It blends state authority with industry responsibility to re-territorialize the online space as a safe space for Australians, extending domestic jurisdiction into the global sphere (Alexander, 2022). This ambition, however, gives rise to a paradox of sovereign overreach: to be effective nationally, the regulator must assert its authority globally, leading to direct conflict with the world's most powerful technology companies and raising critical questions about jurisdiction, free speech, and the future of a unified global Internet.

The *material components* include the platforms' content moderation algorithms, the eSafety Commissioner's portal for reporting abuse, and the technical mechanisms for "geo-blocking" or global removal. The core institutional component is the Office of the eSafety Commissioner itself, an independent statutory body with a significant budget and staff of 125 by 2023, consisting of investigators, lawyers, and technology experts. Its material power is expressed through potent legal tools, including legally binding removal notices for harmful content, blocking orders directed at internet service providers, and the authority to demand and enforce industry codes and standards (Smith et al., 2024).

The *expressive components* are anchored in the Online Safety Act 2021 (OSA). The dominant discourse is "Safety by Design" and the protection of children and adults from cyber-abuse, image-based abuse, and abhorrent violent conduct. The Basic Online Safety Expectations (BOSE) Determination 2022 formalizes these norms, expecting providers to take "reasonable steps" to minimize harm. This dominant discourse is met with powerful counter-narratives from platforms, civil liberties groups, and international critics, who raise concerns about threats to free speech, the risk of creating a "splinternet" by fragmenting the global internet, and the potential for government censorship (Martin, 2025).

The eSafety assemblage is a clear attempt by the Australian state to re-territorialize the digital public sphere, to impose a set of national norms and standards on what has often been seen as a borderless and ungovernable space. The OSA 2021 empowers the Commissioner to issue removal notices for "Class 1" (e.g., child sexual abuse, terrorism) and "Class 2" material. The law imposes civil penalties (up to 500 penalty units) on platforms that fail to remove content within 24 hours (Smith et

al., 2024). This assemblage attempts to extend this territory globally. In the wake of the 2024 Wakeley church stabbing, the Commissioner issued a removal notice to X Corp (formally Twitter) to remove violent footage globally, arguing that geo-blocking for Australians was insufficient because users could bypass it via VPNs. This was a clear attempt to assert that Australian safety standards should define the global accessibility of specific content.

However, this re-territorialization met with fierce *deterritorializing* resistance. X Corp challenged the global takedown order in the Federal Court, arguing that one nation cannot dictate global content standards (calling it "global censorship"). X Corp complied only with geo-blocking, which the Commissioner argued was porous. The existence of Virtual Private Networks (VPNs) proved to be a material deterritorializing force: users can effectively "move" their virtual location, rendering the state's digital borders permeable. In mid-2024, the eSafety Commissioner dropped the Federal Court case against X Corp (Taylor, 2024), choosing instead to focus on the Administrative Appeals Tribunal process and an independent review of the Act. This episode highlighted the limits of the state's territorial reach when confronted by a transnational corporate assemblage that operates according to its own logic of "free speech" and global uniformity.

Australia's co-regulatory safety assemblage exposes the practical limits of national digital sovereignty in a globally integrated platform environment. Although the eSafety Commissioner possesses expansive statutory authority, its effectiveness ultimately depends on the compliance of transnational platforms operating across jurisdictions. The Wakeley case illustrates how technological circumvention and corporate resistance can hollow out formal legal power without directly defying it. Authority in this assemblage is continually asserted and contested rather than conclusively enforced. Australia's experience highlights how safety-oriented digital regulation increasingly operates at the edge of jurisdictional feasibility.

Cross-Case Analysis and Comparison

Synthesizing the findings from these three disparate cases allows the development of a more nuanced theoretical understanding of the paradoxes that define our contemporary digital order. Across India, Brazil, and Australia, governance outcomes are shaped not by formal institutional design alone but by how legal authority, technological systems, organizational capacity, and public discourse are assembled and held together over time. Rather than convergence, the cases display patterned variation shaped by distinct territorial logics and their associated contradictions.

Table 1 summarizes the core characteristics of each assemblage, including their dominant logics, key material and expressive components, and principal territorializing and deterritorializing processes. The comparison highlights that each assemblage stabilizes authority in a different way and, in doing so, generates a characteristic paradox.

Table 1. Comparison of Three Types of Digital Governance Assemblages

Dimension	The Biometric State Assemblage (India)	The Multi-Stakeholder Rights Assemblage (Brazil)	The Co-Regulatory Safety Assemblage (Australia)
Primary Logic	State Control & Efficiency	Civic Rights & Participation	National Safety & Sovereignty
Material Components	Biometric database (CIDR), scanners, APIs, Aadhaar number.	Legal text (Marco Civil), online consultation platforms, internet infrastructure.	Online Safety Act, eSafety Commissioner (institution), removal notices, platform algorithms.
Expressive Components	Discourse of "welfare," "inclusion," "anti-fraud"; counter-discourse of "surveillance."	Principles of net neutrality, privacy, free speech; discourse of "Internet Constitution."	Discourse of "online safety," "duty of care"; counter-discourse of "free speech," "censorship."
Territorializing Process	Mandatory linking to services; centralization of identity data under UIDAI.	Participatory law-making; codification of rights into law.	Granting of strong regulatory powers; issuance of binding global takedown orders.
Deterritorializing Process	Technical failures, data breaches, privacy lawsuits, citizen resistance.	Corporate lobbying, conflicting constitutional law, judicial weakening of principles.	Platform resistance, technological circumvention, jurisdictional legal challenges.
Central Paradox	**Frictional Inclusion—** A system designed for frictionless inclusion creates new, severe frictions for the most vulnerable.	**Normative Fragility—** A normatively powerful rights framework is easily undermined by stronger material and institutional forces.	**Sovereign Overreach—** National effectiveness is perceived to require global control, leading to jurisdictional conflict.

First, the cases vividly demonstrate the contingency of power. Power is not a static attribute possessed by an actor like "the state" or "a corporation," but is an emergent property of a specific assemblage's configuration. The Indian state's immense power through Aadhaar is entirely contingent on its technological infrastructure functioning correctly; but when a fingerprint scanner fails, that power evaporates for the individual at that moment. The power of Brazilian civil society was potent during the legislative process of the Marco Civil, where the participatory assemblage gave its voice weight, but this power diminished once the contest shifted to judicial and corporate arenas where civil society had far less influence. Similarly, the Australian regulator's formidable legal power is contingent on its practical ability to enforce its will against global corporations that can mobilize vast legal and technical resources to resist.

Second, all three cases reveal a deep underlying paradox of territorialization. In each instance, actors deploy deterritorializing technologies—global platforms, centralized databases, the internet itself—to achieve classic Westphalian goals of territorial control. India seeks to territorialize its population into a single database. Brazil sought to territorialize its digital space as a domain of rights. Australia seeks to territorialize its legal jurisdiction by extending it globally. This fundamental contradiction—attempting to draw hard boundaries on a borderless medium—is a primary engine of instability and conflict. Sassen's (2008) insight that national capabilities are being repurposed for a global age is evident here: the nation-state is using its traditional tools of law and administration to grapple with a phenomenon that fundamentally challenges its territorial basis.

Third, the analysis underscores the politicization of the technical. Seemingly neutral technical architectures and standards are, in fact, intensely political sites where governance is enacted and contested. The biometric standards of Aadhaar are not just technical specifications; they are political decisions that determine who is included and excluded from the state. The principle of net neutrality in the Marco Civil is not just a network management rule; it is a political commitment to a particular vision of an open and equitable internet. The content moderation algorithms targeted by Australia's eSafety Commissioner are not just code; they are opaque systems that exercise enormous power over public discourse. The adage that "code is law," as articulated by Lessig (1999), is more than a slogan – it is an empirical reality across these assemblages. The material and expressive components of these assemblages are locked in a dynamic feedback loop, where law attempts to shape technology, and technology constantly redefines the boundaries of what is politically and legally possible.

Conclusion

This article has applied an assemblage-based approach to the study of digital governance, moving beyond static typologies and regime-centered analyses. By examining how heterogeneous elements—technologies, laws, institutions, and discourses—are assembled in practice, the paper reframes digital governance as a contingent and contested process rather than a settled institutional order.

The comparative analysis of India's Aadhaar system, Brazil's Marco Civil da Internet, and Australia's eSafety Commissioner identifies three recurrent paradoxes. *Frictional inclusion* in India shows how systems designed to streamline access can generate new exclusions when technological mediation fails. *Normative fragility* in Brazil demonstrates that rights-based frameworks, while symbolically powerful, remain vulnerable when enforcement capacity and material infrastructure do not fully support them. *Sovereign overreach* in Australia highlights how national regulators face structural limits when attempting to govern globally integrated platforms. These paradoxes are not simply implementation failures; they reflect deeper tensions involved in governing a deterritorialized digital environment through territorially grounded institutions.

The findings carry significant implications for both scholars and practitioners. First, digital governance capacity cannot be inferred from formal legal authority alone. Effective governance depends on the alignment of legal mandates with technical systems and organizational resources (Milakovich, 2021; Xin et al., 2025). Second, governance frameworks must be adaptive rather than static. As technologies evolve, regulatory arrangements require ongoing recalibration rather than one-time design (Xin & Wang, 2025). Third, contestation should be treated as a normal condition of digital governance. Attempts to suppress conflict often displace it into technical or jurisdictional domains, where it becomes less visible but no less consequential.

For public administration practice, the findings suggest the value of governance approaches that are both polycentric and iterative (Morrison et al., 2023). Multi-actor coordination, as seen in Brazil's participatory model, can enhance legitimacy but must be matched with institutional capacity to sustain outcomes over time. Embedding public values into system design—through procurement standards, auditing mechanisms, and accountability requirements—can help mitigate exclusionary effects such as those observed in Aadhaar. Regulatory sandboxes and experimental oversight arrangements may offer additional flexibility in domains characterized by rapid technological change.

This study, being exploratory, has certain limitations. First, it relies on secondary data sources, meaning that our analysis is constrained by available documentation and may overlook on-the-ground perspectives. Second, the three cases, while diverse, do not cover all possible digital governance contexts, so generalizability is limited. The aim is theoretical inference rather than broad empirical generalization, and readers should be cautious in extending the findings to other contexts. Third, policies and technologies continue to evolve even as this manuscript is being written. The assemblages described here are subject to change, and some observations may become outdated. We have noted where recent developments (e.g., new legislation or technological changes in 2024–25) might alter the assemblage dynamics. Despite these limitations, the study provides a baseline understanding that future research can build upon with more data and additional cases.

References

Alexander, S. (2022). A Uniquely Australian Approach: A Thematic Analysis of the Normative Foundations of Australia's Approach to The Regulation of The Internet. *Adelaide Law Review, 43*(1), 345-375.

Alter, K. J. (2022). The promise and perils of theorizing international regime complexity in an evolving world. *The Review of International Organizations, 17*(2), 375-396. https://doi.org/10.1007/s11558-021-09448-8

Baer, M., & Gerlak, A. (2015). Implementing the human right to water and sanitation: a study of global and local discourses. *Third World Quarterly, 36*(8), 1527-1545. https://doi.org/10.1080/01436597.2015.1043993

Banerjee, S. (2016). Aadhaar: Digital inclusion and public services in India. *World Development Report 2016: Background Paper Digital Dividends* (pp. 81-92). World Bank Group.

Bennett, A., & Checkel, J. T. (2014). *Process tracing and the social sciences: From metaphor to analytic tool.* Cambridge University Press.

Borah, P. P., & Bhuyan, A. J. (2024). Living with the Aadhaar: India's Changing Contours of Identity and Governance. *Indian Journal of Public Administration, 70*(3), 615-620. https://doi.org/10.1177/00195561241257460

Bridge, G. (2021). On pragmatism, assemblage and ANT: Assembling reason. *Progress in Human Geography, 45*(3), 417-435. https://doi.org/10.1177/0309132520924710

DeLanda, M. (2006). Deleuzian social ontology and assemblage theory. In M. Fuglsang & B. M. Sorensen (Eds.), *Deleuze and the Social* (pp. 250-266). Cambridge University Press.

DeLanda, M. (2016). *Assemblage theory*. Edinburgh University Press.

Deleuze, G., & Guattari, F. (1980). *Mille plateaux (Vol. 4).* éd. de Minuit.

Drezner, D. W. (2009). The Power and Peril of International Regime Complexity. *Perspectives on politics, 7*(1), 65-70. https://doi.org/10.1017/S1537592709090100

Fratini, S., Hine, E., Novelli, C., Roberts, H., & Floridi, L. (2024). Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models. *Digital Society, 3*(3), 59. https://doi.org/10.1007/s44206-024-00146-7

Freedom House. (2021). *Brazil: Freedom on the Net 2021 (country report)*. https://freedomhouse.org/country/brazil/freedom-net/2021

Hoskins, G. T. (2018). Draft Once; Deploy Everywhere? Contextualizing Digital Law and Brazil's Marco Civil da Internet *Television & New Media, 19*(5), 431-447. https://doi.org/10.1177/1527476417738568

Jain, M. (2019). *The Aadhaar Card: Cybersecurity Issues with India's Biometric Experiment.* Univeristy of Washington. https://jsis.washington.edu/news/the-aadhaar-card-cybersecurity-issues-with-indias-biometric-experiment/

Katzenbach, C., & Ulbricht, L. (2019). Algorithmic governance. *Internet Policy Review, 8*(4), 1–18. https://doi.org/10.14763/2019.4.1424

Khera, R. (2017). Impact of Aadhaar on welfare programmes. *Economic and Political Weekly, 52*(50), 61-70.

Kornberger, M., Pflueger, D., & Mouritsen, J. (2017). Evaluative infrastructures: Accounting for platform organization. *Accounting, Organizations and Society, 60*, 79-95. https://doi.org/10.1016/j.aos.2017.05.002

Legg, S. (2011). Assemblage/apparatus: using Deleuze and Foucault. *Area, 43*(2), 128-133. https://doi.org/10.1111/j.1475-4762.2011.01010.x

Lessig, L. (2009). *Code: And Other Laws of Cyberspace*. ReadHowYouWant.com.

Marcus, G. E., & Saka, E. (2006). Assemblage. *Theory, culture & society, 23*(2-3), 101-106. https://doi.org/10.1177/0263276406062573

Martin, N. (2025). Online safety regulation of deepfake abuse: a case study on Australia's eSafety Commissioner. *Griffith Law Review, 34*(1), 23-46. https://doi.org/10.1080/10383441.2025.2504791

Masiero, S., & Shakthi, S. (2020). Grappling with Aadhaar: Biometrics, Social Identity and the Indian State. *South Asia Multidisciplinary Academic Journal*, *23*. https://doi.org/10.4000/samaj.6279

Meng, W., Wang, F., & Xin, G. (2024). Making agile governance work: the community grid as a 'safety valve' institution during the COVID-19 pandemic. *Journal of Chinese Governance, 9*(2), 197-220. https://doi.org/10.1080/23812346.2024.2332005

Milakovich, M. E. (2021). *Digital governance: Applying advanced technologies to improve public service*. Routledge.

Morrison, T. H., Bodin, Ö., Cumming, G. S., Lubell, M., Seppelt, R., Seppelt, T., & Weible, C. M. (2023). Building blocks of polycentric governance. Policy Studies Journal, 51(3), 475-499. https://doi.org/10.1111/psj.12492

Müller, M. (2015). Assemblages and Actor-networks: Rethinking Socio-material Power, Politics and Space. *Geography Compass, 9*(1), 27-41. https://doi.org/10.1111/gec3.12192

Neto, J. A. M. (2018). *The Operation of Multistakeholderism in Brazilian Internet Governance: Governance Innovation through Multistakeholderism Generativity.* University of Kent.

Onlyias. (2023). *Massive Aadhaar Data Breach Of 815 Million Indians.* https://pwonlyias.com/current-affairs/aadhaar-data-breach/

Phillips, J. (2006). Agencement/Assemblage. Theory, Culture & Society, 23(2-3), 108-109. https://doi.org/10.1177/026327640602300219

Plantin, J. C., Lagoze, C., Edwards, P. N., & Sandvig, C. (2018). Infrastructure studies meet platform studies in the age of Google and Facebook. *New media & society, 20*(1), 293-310. https://doi.org/10.1177/1461444816661553

Rodriguez, K., & Pinho, L. (2015). *Marco Civil Da Internet: The Devil in the Detail.* Electronic Frontier Foundation.

Sassen, S. (2008). *Territory, authority, rights: From medieval to global assemblages.* Princeton university press.

Sautchuk-Patrício, N. (2022). *Revisiting net neutrality from a polycentric perspective: Brazilian and German scenarios (No. 31).* Global Cooperation Research Papers.

Savage, G. C. (2020). What is policy assemblage?. *Territory, Politics, Governance, 8*(3), 319-335. https://doi.org/10.1080/21622671.2018.1559760

Singh, P. (2021). Aadhaar and data privacy: biometric identification and anxieties of recognition in India. *Information, Communication & Society, 24*(7), 978-993. https://doi.org/10.1080/1369118X.2019.1668459

Smith, M., Nolan, M., & Gaffey, J. (2024). Online safety and social media regulation in Australia: eSafety Commissioner v X Corp. *Griffith Law Review, 33*(1), 2-18. https://doi.org/10.1080/10383441.2024.2405760

Steibel, F. (2012, October 22-25). *Designing online deliberation using web 2.0 technologies: drafting a bill of law on internet regulation in Brazil* [Paper Presentation]. ICEGOV '12: Proceedings of the 6th International Conference on Theory and Practice of Electronic Governance. New York, United States. https://doi.org/10.1145/2463728.2463738

Taylor, J. (2024). *X says "free speech has prevailed" after eSafety commissioner drops case over Wakeley church attack posts.* The Guardian. https://www.theguardian.com/technology/2024/jun/05/x-elon-musk-vs-australia-esafety-commissioner-wakeley-church-stabbing-footage

Xin, G., Cui, J., Wang, F., & Zhang, J. (2025). Demystifying digital economic performance in China: A local officials' career incentive perspective. *International Public Management Journal, 28*(6), 747-769. https://doi.org/10.1080/10967494.2025.2474512

Xin, G., Esembe, E. E., & Chen, J. (2023). The mixed effects of e-participation on the dynamic of trust in government: Evidence from Cameroon. *Australian Journal of Public Administration, 82*(1), 69-95. https://doi.org/10.1111/1467-8500.12569

Xin, G., & Huang, J. (2025). Making the people's voice heard: pathways of E-participative governance in China. *Journal of Chinese Governance, 10*(1), 33-56. https://doi.org/10.1080/23812346.2024.2400634

Xin, G., & Wang, Y. (2025). The Algorithmic Leviathan and the Digital Polis: A Review of Global Digital Governance Dilemmas and Pathways. *Chinese Journal of International Review, 7*(2), 2550006. https://doi.org/10.1142/S2630531325500064

Yeung, K. (2018). Algorithmic regulation: A critical interrogation. *Regulation & governance, 12*(4), 505-523. https://doi.org/10.1111/rego.12158

Yin, R. K. (2018). *Case study research and applications (Vol. 6)*. Sage Publishing.