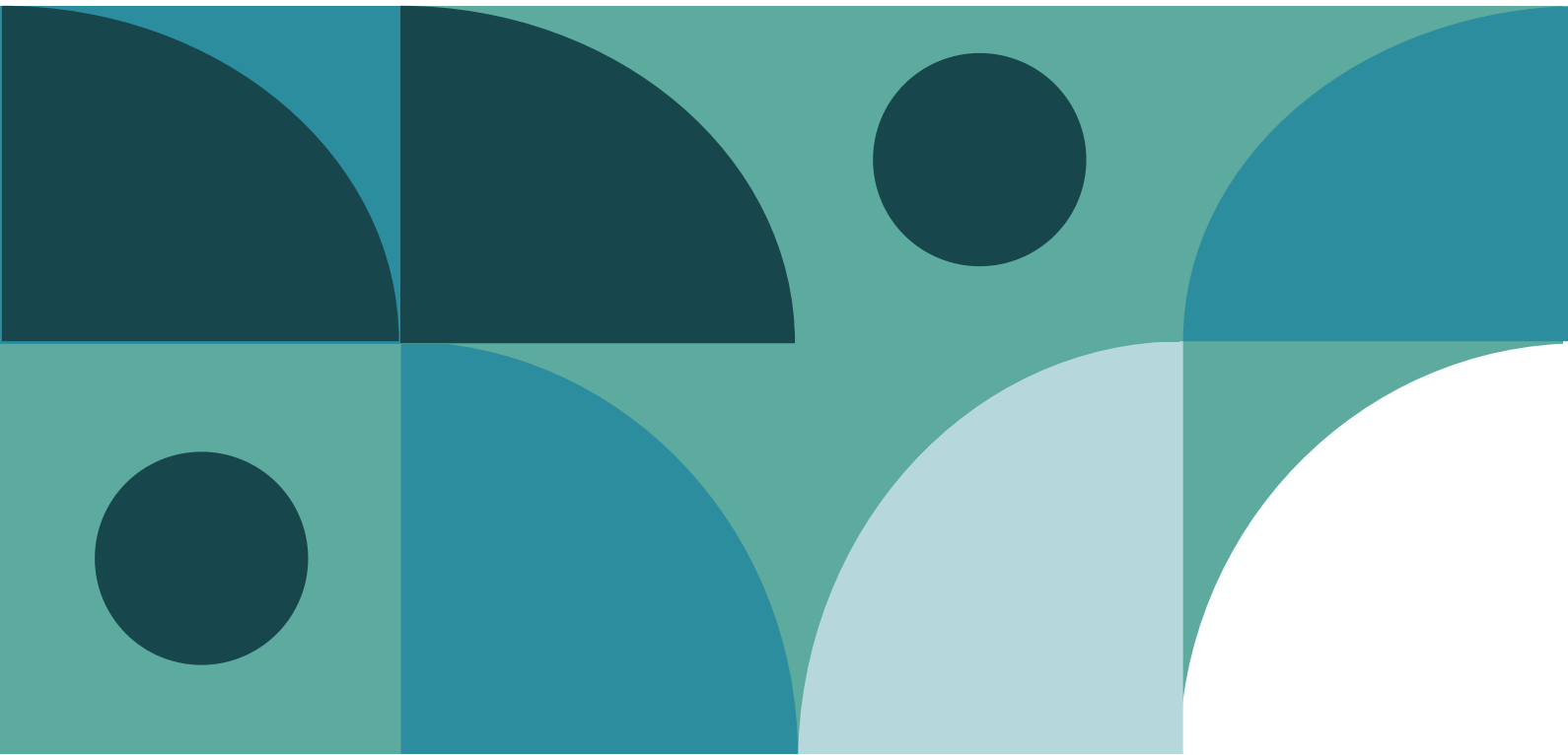
TECHGLOBAL INSTITUTE

Regional Power, Policy Shaping and Digital Futures:

Norm Externalization through the Delhi and Beijing Effects

Diyi Liu and Shashank Mohan

July 2025



TECHGLOBAL INSTITUTE

www.techglobalinstitute.com

Table of Contents

01
INTRODUCTION

04
THE BRUSSELS EFFECT

08
THE BEIJING EFFECT

13
THE DELHI EFFECT

18
FUTURE OF GLOBAL TECHNOLOGY GOVERNANCE

Introduction

From the early internet's libertarian ethos – emblematized by John Perry Barlow's 1996 *Declaration of Independence of Cyberspace* proclaiming that governments "have no sovereignty where we gather" – to today's intensely contested global regulatory landscape, internet governance has undergone a remarkable transformation. The once-dominant vision of an ungovernable cyberspace has yielded to competing national and regional frameworks that now actively shape our digital experiences. As the internet became centralized, and platform companies expanded across borders, global technology governance emerged as a central focus of academic and policy debate. Scholars have mapped these divergent approaches through various taxonomies – from the "Four Internets" identifying Silicon Valley's innovation-driven Open Internet, the EU's rights-centric Bourgeois Internet, DC's market-oriented Commercial Internet, and China's state-controlled Paternal Internet, to newer frameworks analyzing models of digital sovereignty. Each governance model operates across the internet's full stack: from the physical infrastructure layer, through the code and protocol layer, to the information layer where content flows and user interactions occur.

As the world becomes increasingly interconnected, the rules and norms governing technology no longer remain confined to their jurisdictions of origin. Instead, they ripple outward, creating what scholars have labelled national and regional *effects* that reflect both governance philosophies and geopolitical ambitions. They represent the process of norm externalization – whereby regulations, standards, and governance approaches developed in one jurisdiction influence or are adopted by others, either through market mechanisms, deliberate policy diffusion, or in response to capacity constraints and power asymmetries. These effects are not

merely academic constructs, but powerful forces reshaping the global digital order: They enable mapping pathways of policy transfer across borders, and shed light on how external influences interact with domestic politics in regulatory outcomes. Further, norm externalization characterizes geopolitical influence and economic and technological leverage of exporting countries, and reveals normative alignments between socio-political systems that seek to adopt these governance models. When the European Union (EU) implements stringent data protection standards through the General Data Protection Regulation (GDPR), companies worldwide often find it more efficient and cost-effective to apply these standards globally rather than maintain separate systems for each jurisdiction, as witnessed when Microsoft extended GDPR rights to all users worldwide. As China extends its Digital Silk Road (DSR) through infrastructure investments across the Majority World (e.g., the cross-border cable projects), its technological standards and governance approaches could be transferred to recipient countries. Similarly, as India develops and exports its digital public infrastructure (DPI), it exerts influence over other countries in the Majority World to adopt similar population-wide digital welfare schemes that are based on open-standards and operationalize interoperability.

Such extraterritorial impacts also create profound implementation challenges. For instance, the compliance requirements in the EU for platforms necessitate dedicated resources for content moderation and standardized reporting mechanisms in the region; data localization demands in multiple jurisdictions might strain seamless global service delivery models; and privacy protection standards vary dramatically across regions. The competition between different regulatory models is particularly consequential for countries in the Majority World, which find themselves navigating competing governance frameworks while attempting to assert their own digital sovereignty. As Majority World countries seek technological advancement, the regulatory governance they adopt increasingly reflects broader geopolitical alignments and values. Due to

capacity constraints to undertake detailed studies on drafting and formulating tech regulation, when other jurisdictions with similar political or demographic systems create regulations, it becomes easier to find linkages and adopt them, either wholly or in modified form, rather than invest in developing local expertise. This policy learning takes various forms: some countries become adopters who largely import frameworks, others emerge as hybridizers who blend approaches, while a few act as innovators creating unique models. Countries may also align their laws with others to remain favorable for trade and geopolitical relationships. Moreover, formal capacity building programs — from the EU's Digital4Development initiatives to technical assistance from international organizations – further facilitate learning and alignment.

While regulatory externalization has been well analyzed in the context of the EU, particularly through the well-established *Brussels Effect*, the enabling conditions and mechanisms of influence from two emerging global powers – China and India, representing a third of the global population – remain underexplored in global policy discourse. Moreover, different forms of norm externalization beyond adoption of formal regulatory standards are still insufficiently studied. This essay seeks to address these gaps by examining the conditions and mechanisms through which the Beijing Effect and the Delhi Effect might manifest. First, the tech-developmental models embraced by both countries, which enable initiatives like China's DSR and India's DPI focusing on digital infrastructure, create demonstrable frameworks that address concrete development needs in recipient countries. Second, both China and India's strategic positioning as sovereignty-centered alternatives challenging Global North dominance greatly aligns with many Majority World countries' own aspirations. Third, shared history, cultural associations, and – particularly in the case of India and South and Southeast Asia – postcolonial resistance create ideological alignment that facilitates norm adoption beyond mere technical considerations. Finally, the adaptive, non-binding implementation approaches in the Beijing Effect and the Delhi Effect offer greater flexibility and feasibility compared to

the adoption of stringent regulatory standards, particularly valuable for countries with limited regulatory capacity. By comparing these two effects with the Brussels Effect, the analysis reveals how different governance approaches translate into distinct pathways of norm externalization, with profound implications for whose values and priorities will shape the collective digital future, particularly in the Majority World.

The Brussels Effect

Over the last two decades, the EU stands as perhaps the world's most influential regulatory power in the digital sphere, projecting what legal scholar Anu Bradford famously termed the "Brussels Effect." Unlike traditional forms of influence that rely on military might or economic incentives, the EU wields significant market-based regulatory power that travels through global markets, transforming how technologies function worldwide. Through landmark legislations – including the General Data Protection Regulation (GDPR), the Digital Services Act (DSA), the Digital Markets Act (DMA), and the Artificial Intelligence Act (AI Act) – the EU has established itself as the world's preeminent regulatory standard-setter. The EU's rights-based approach consistently frames requirements in terms of protecting fundamental rights: privacy rights in GDPR, consumer protections in product regulations, and various risk-based safeguards in the AI Act. Beyond digital markets, the EU extends its regulatory reach to corporate accountability, environmental and climate regulation, food safety and agricultural standards, and financial regulations.

Enabling Conditions

Bradford's analysis identifies five interdependent conditions that enable the Brussels Effect: market size and power, regulatory capacity, stringent standards, inelastic targets, and non-divisibility of standards. With approximately 450 million affluent consumers and US$41,423 GDP per capita in 2023, the EU possesses economic leverage few global companies can ignore. This market power is complemented by sophisticated regulatory institutions with extensive sanctioning authority.
For instance, GDPR violations can trigger penalties up to 4% of global turnover, while competition law

breaches carry fines up to 10% of annual revenue. Between 2017 and 2019, in the EU, Google faced cumulative fines amounting to US$9.5 billion, while more recent actions against LinkedIn (US$325 million), Meta (US$ 2.1 billion), and Apple (US$2.01 billion) demonstrate the EU's commitment to enforcement.

More recently, the Commission fined Meta and Apple in breach of the DMA (nearly US$800million). Beyond financial penalties, EU regulators have proven willing to block non-compliant services entirely, as evidenced by Italy's suspension of DeepSeek's chatbot over data privacy concerns. Unlike the United States' neoliberal regulatory approach, the EU has demonstrated consistent political will to deploy its regulatory capacity toward stringent rules, favoring government intervention to preempt market failures through strong ex-ante regulation. Further, the EU's regulations target consumer markets where businesses have limited mobility and must comply with local rules to maintain access. Finally, when corporations find it not legally, technically, or economically feasible to maintain different compliance models for different markets, they adopt the strictest standards globally – though this non-divisibility is not absolute, as shown by Microsoft's unbundling of Teams in Europe and Google News' temporary withdrawal from Spain.

Mechanisms of influence

The Brussels Effect operates through two primary mechanics. Expanding on the *California Effect* – a concept introduced by David Vogel to describe the "race to the top" in corporate environmental regulations within the U.S. federal system – Bradford outlines the de facto effect, wherein non-EU firms voluntarily adopt EU standards globally (e.g. Apple adopted USB-C charging port for iPhone models after years of battle with the EU). This occurs because maintaining separate regulatory systems for different markets is often impractical.

Meanwhile, the *de jure* effect manifests when other jurisdictions formally adopt laws mirroring EU standards. GDPR has inspired similar legislative initiatives globally, including the California Consumer Privacy Act and Brazil's General Data Protection Law. Similarly, the EU's

DSA has influenced Brazil's approach to disinformation through the country's Bill No. 2630/2020 and may inspire others, for instance countries in the African continent to adopt similar laws. This legislative ripple effect demonstrates how EU regulations serve as influential templates for countries developing their own regulatory frameworks. The phenomenon is particularly pronounced in Majority World countries, where administrative agencies have fewer resources to develop completely original regulatory frameworks. Beyond the *de facto* and *de jure* effect, the EU also extends its regulatory influence through leading international standard setting, technical assistance, and capacity building with other countries.

Limitations and Challenges of the Brussels Effect

Despite its considerable influence, the *Brussels Effect* faces important limitations that reveal both its constraints, and the emergence of alternative models of norm externalization. On the *de facto* effect, empirical research on the influence of EU laws on data privacy policies suggests that many US online services maintain differentiated approaches between EU and US users, indicating that the costs of regulatory differentiation may be lower than commonly assumed, especially for technology services. More recently, companies designated under the DMA and DSA have increasingly pursued legal action against EU institutions, revealing stronger resistance when stringent regulations directly impact core business models.

More significantly, power import markets like China and India are actively challenging the de facto effect through their own market leverage, forcing global companies to make exceptions in these two countries. For example, as the world's second-largest consumer market and the largest smartphone market, China demonstrates how hardware and services can be reconfigured for specific markets while maintaining core technological standards. As a result, many global companies offer localized services in China and India to suit local laws and policies for sustained access to these markets. Apple, for instance, announced planned collaborations with Alibaba and Baidu for AI features specifically for the Chinese

market. Similarly, online content companies like YouTube, Instagram, and X abide by India's heavy censorship orders that are confidential in nature. Companies often don't transfer strict standards, especially when they are based on software adjustments to other regions too, for instance Apple allows for third-party apps stores on its devices only in the EU, further illustrating the divisibility of standards.

On the de jure effect, while the data protection frameworks have diffused to many jurisdictions, they also undergo significant adaptations. Moreover, so far this diffusion is less evident in emerging domains like artificial intelligence regulation, where pressure from both Silicon Valley's leading AI market players and alternative industry policies from countries like China create competing influences. Similarly, as we will discuss in this essay later, countries like India are blunting even the *de jure* Brussels Effect due to localized factors like economic and capacity constraints.

These limitations point to our main argument: not only do emerging powers like China and India challenge the efficacy of the *Brussels Effect*, but the conditions identified under the theoretical framework might not fully account for alternative pathways of norm externalization increasingly witnessed from these two countries. In the following sections, we examine how China and India deploy alternative strategies that operate through infrastructure development, digital sovereignty appeals, and ideological alignment, as well as the implications for the Majority World.

The Beijing Effect

While the EU wields the power of market access and regulatory capacity to globalize its regulatory frameworks, China has pioneered a different approach to extending digital influence. The so-called *Beijing Effect*, originally coined alongside the Brussels Effect by Bradford, and later reconceptualized by legal scholars Matthew Erie and Thomas Streinz, represents China's strategy for shaping global digital governance through infrastructure deployment, technical standards, and a sovereignty-centered vision that resonates particularly in the developing world.

Economic leverage and infrastructure-first approach

The foundation of the Beijing Effect lies in China's unique model of tech-developmental capitalism where state oversight, content control, technological self-sufficiency, and economic development work in concert. China's digital strategy mobilizes both private and state-owned capital under the shared aim of national technological advancement, which creates powerful export capabilities and distinct advantages in global digital markets. It partly explains why Chinese technology companies consistently offer more cost-effective solutions than Western alternatives – making comprehensive digital transformation financially viable for countries with limited resources. On top of project-related policy bank funding, state-owned banks provided companies like ZTE and Huawei generous financial support. Under the DSR umbrella, these companies have often been able to offer equipment up to 30-40% cheaper than Western suppliers. The state-market coordination translates directly into competitive advantages in developing markets.

The *Beijing Effect* manifests most visibly through China's DSR, under the Belt and Road Initiative (BRI), which extends digital connectivity

across Asia, Africa, and beyond through telecommunications networks, data centers, and e-commerce platforms. Instead of a specific government initiative, the DSR has evolved into an umbrella term for China's broader vision of governing the global digital sphere, achieved largely through the strategic activities of China's domestic tech giants and ICT industry.

Unlike the EU's regulatory packages which operate through formal legal mechanisms, the DSR creates pathways for influence through physical investments and technical implementations. This infrastructure-first approach establishes China's digital standards at the foundational level of internet architecture, creating long-term influence that operates beneath the more visible layer of formal regulations.

Specifically, China provides physical infrastructure – fiber optic cables, cellular networks, and computing facilities – that forms the backbone of emerging digital economies. The Pakistan-China Fibre Optic Project exemplifies this approach, enhancing Pakistan's internet capacity while creating infrastructure operated by Chinese firms. This physical foundation and network architecture embodies certain technical standards that shape subsequent governance decisions among local regulators. Similarly, Huawei plays a crucial role in Africa's telecom network, including 70% of the continent's 4G network. The scale of this infrastructure-based influence is remarkable. Huawei has deployed 5G infrastructure across countries like Kenya and South Africa. Together with ZTE, they have deployed more than 350 smart city projects in over 60 countries, including the Philippines, Pakistan, and Malaysia. In Ethiopia, Huawei created campus networks, established cloud services and micro data centers in Addis Ababa that serve as the backbone for government sectors and educational institutions. Through the establishment and export of technical standards via infrastructure projects, China creates enduring pathways for long-term influence over global digital systems, promoting a governance model that emphasizes stability, development, and state authority.

Moreover, building upon this physical

infrastructure is an integrated ecosystem of technologies and services, driven by leading private companies such as Baidu, Tencent, and Alibaba (BAT). For instance, Alibaba's investment in Lazada, a Singapore-based e-commerce giant dominant across Thailand, Malaysia, and Vietnam, demonstrates how Chinese firms integrate into local economies in Southeast Asia. As Lazada became the largest e-commerce operator in South and Southeast Asia, it also adopted Alibaba's technical infrastructure systems (e.g. cloud and data management), reinforcing China's influence over transnational data governance. The mechanisms of influence thus manifest through multiple layers building on the infrastructure-first approach: At the application layer, Chinese platforms bring data practices and content standards that might carry on domestic regulatory preferences. At the business operations layer, mergers and acquisitions integrate local digital economies into China's interacted systems, creating lasting dependencies that extend beyond the immediate technical infrastructure. At the data architecture layer, cloud services establish protocols for information storage and processing that follow Chinese governance models.

Sovereignty appeals, ideological alignment, and development aspirations

China's approach to digital governance prioritizes state sovereignty in cyberspace over universal rights frameworks, creating natural appeal for governments seeking greater control over their digital domains. For instance, while China has adopted EU-inspired data protection mechanisms, research has argued that Personal Information Protection Law 2021 represents a strategic instrumentalization of the GDPR to shape its unique data protection landscape, with a strong data localization approach. Moreover, China's expanding export control regime – which includes technologies and services related to national security –has significantly strengthened its economic security. For instance, this has created barriers for companies like ByteDance, TikTok's parent company, to sell the platform's algorithms, which are likely classified under restricted technologies. This sovereignty-centered approach has

found receptive audiences across developing regions. Countries like Indonesia, Bangladesh, Pakistan, and Vietnam have adopted or proposed similar data localization approaches, which carry significant economic ramifications. The emphasis on sovereignty appeals to governments seeking greater control over their digital domains.

The spread of internet management technologies further illustrates this alignment. For instance, since 2018, reports indicate that Pakistan has been testing a web monitoring system built upon technology from Canada-based company Sandvine, utilizing Deep Packet Inspection to monitor communications and analyze traffic patterns. Recent reports from 2024 further confirm that the Pakistani government has transitioned to a firewall-like system deploying Chinese technology, resulting in persistent internet slowdowns and service disruptions. Cambodia's adoption of a national CCTV system for security purposes exemplifies how alignment with China's governance vision facilitates technology adoption that extends beyond mere economic considerations.

Further, China's digital governance model draws additional strength from a historical-cultural vision challenging Western digital dominance. As a developing country that successfully achieved technological advancement, China offers a narrative that resonates with nations pursuing similar trajectories.

Adaptive instruments facilitating adoption

A crucial distinction, as noted by Erie and Streinz, from the Brussels Effect lies in implementation flexibility. While EU regulations often impose rigid compliance requirements, the Beijing Effect operates through more adaptive, non-binding instruments, such as agreements on DSR cooperation or investment, that can be tailored to local contexts, as well as technical standard setting where a number of global companies have subject themselves to. This approach proves effective in countries like Kazakhstan, where research has shown how the mobile telecommunication sector has been seeking digital development while maintaining regulatory autonomy to counterbalance geo-political disruptions. Countries in the Gulf have also "actively shaped the

engagement of tech giants within their countries, ensuring alignment with their national objectives." This adaptability allows for customization to local political and cultural contexts while still advancing China's broader strategic objectives. As China continues to develop and implement AI regulations domestically, it is transforming itself into a laboratory for governance experiments that may subsequently influence how emerging technologies are regulated across its sphere of influence.

The *Beijing Effect* ultimately offers a demonstrable developmental model that addresses immediate infrastructure gaps while respecting state sovereignty concerns. Developing nations confront significant digital divides and infrastructure deficiencies that Chinese investments directly address with immediate, tangible benefits that normative regulatory frameworks cannot match. In other words, the pragmatic focus on economic growth and technological advancement aligns precisely with many developing nations' immediate priorities, providing concrete solutions without imposing explicit political conditionality. Its growing global influence suggests that the future of digital governance may be determined not merely by whose rules are strictest or most comprehensive, but by whose reports indicate that Pakistan has been testing a web monitoring system built upon technology from Canada-based company Sandvine, utilizing Deep Packet Inspection to monitor communications and analyze traffic patterns. Recent reports from 2024 further confirm that the Pakistani government has transitioned to a firewall-like system deploying Chinese technology, resulting in persistent internet slowdowns and service disruptions. Cambodia's adoption of a national CCTV system for security purposes exemplifies how alignment with China's governance vision vision most effectively addresses the concrete needs and aspirations of nations striving for digital transformation.

However, this effectiveness carries significant downsides for digital rights and internet freedom in developing countries, creating a tension between technological advancement and the preservation of digital spaces for the user's sovereignty. Critics have raised concerns about how infrastructure development could subject countries to increased internet surveillance, the challenges of deploying facial-recognition technology without adequate safeguards, and the risks of non-transparent procurement processes.

The Delhi Effect

There's another digital governance model or "digital empire" that has been taking shape in South Asia for decades, with Delhi at its epicenter, slowly charting its own course in a multipolar world – we term this the *Delhi Effect*. Asserting its own digital sovereignty and positioning itself as a new global norm setter, especially in the Majority World, New Delhi has been slowly but steadily crafting its distinct digital governance framework. A hybrid of the pro-innovation US model, state-centric Chinese model, and somewhat rights-focused European model, Delhi is blunting the eponymous *Brussels Effect*. There are two arcs to consider here. First, a shift away from the Brussels effect and the broader Western conceptualization of the global order to position India as a non-aligned technology governance leader. Second, influencing other countries with new standards of technology governance in the form of regulatory norm externalization and DPIs.

Shared colonial histories and aligned values

Delhi's *de jure* effect - a parallel but crucial trend to illustrate is how tech regulations crafted in New Delhi are influencing neighboring countries, for comparable but different reasons to the Brussels Effect. On the heels of mass-protest movements in India, New Delhi introduced stringent rules for online platforms and content governance in 2021 that required vague content takedown obligations, presence of local staff, access to end-to-end encrypted apps, and a mandate to pre-filter certain categories of harmful content. All these obligations are tied to a platform's treasured safe-harbor protection for hosting third-party content, and heavily targeted towards popular social media platforms. Forcing online platforms to comply with stringent rules or take individual battles over content and domestic behavior to court.

Perhaps the most illustrative influence of Indian platform regulation law has been on Bangladesh. Bangladesh's draft rules for OTT platforms published in 2021 are substantially copied and inspired from India's IT Rules, 2021. Indian regulation asking online messaging platforms like WhatsApp and Signal to share information on first-originators of messages has been directly borrowed into Bangladesh's OTT policy. Worryingly, this is an example of a mechanical and un-contextualized transfer, as Bangladeshi laws don't provide for a safe-harbor protection to online intermediaries like India. Other mandates from Indian law about the presence of local officers, and vague terms for content takedowns seem to be common with policies being debated in Bangladesh too. The heavy-handedness over online content continues in other countries. Sri Lanka's Online Safety Act contains over-broad provisions barring communication of "false" statements, and statements causing harassment similar to language adopted by the IT Rules in India. In Pakistan, too, there are laws that permit state agencies to conduct wide surveillance, including web-browsing and encrypted messaging apps.

It is pertinent to lay down that countries in South Asia are characterized by excessive executive control over cyberspace (including outright app bans, with India having blocked TikTok and WeChat and Pakistan blocking X and Telegram), permissive access to data by law enforcement agencies, prevalent cultures around network shutdowns, trends that lean towards data localization, and increasing tendencies to quell mass movements asserting democracy. A shared colonial history between India, Pakistan, and Bangladesh is an influential condition for cross-border transfer. Another condition enabling such regulatory externalization is cultural and demographic associations, wherein governments continue to occupy a paternalistic relationship with their citizens as compared to Western democracies. Where a large section of the citizenry is dependent on their governments for food, shelter, and employment, societal relationships are on a less equal footing, enabling state control. As argued in this article, influence over digital futures will be moderated by motivations to search for alignment in vision and values for self-sufficiency and local cultures in addition to global legal standards set by Europe or California.

Digital self-sufficiency and sovereignty

Beyond regulatory externalization - another unique way (although similar to China's tech developmental capitalism) Delhi is actively exporting its influence in the digital realm through "success" stories around its Digital Public Infrastructure. For about 15 years now, India has been building digital protocols, assets, and technology infrastructure for digitizing various aspects of population-wide public services. It has built interoperable digital systems for identity (Aadhaar), payments (UPI), document verification (DigiLocker), and access to COVID-19 vaccines (CO-WIN), among others. Despite challenges around inclusion and privacy, these DPIs resonate immensely with governments around the world due to their potential for social upliftment and welfare delivery. Multilateral international institutions and coalitions like the UN, World Bank, IMF, and the G20 have enthusiastically promoted the adoption of DPIs, especially for countries in the Majority World and have championed India's adoption of population-scale DPIs. India, through conveningslike the G20, has aggressively pushed for adoption of its DPI models across the world, trying to occupy a position of leadership in development and adoption globally. The upcoming India AI Summit will give it another opportunity to celebrate its DPI model and demonstrate its technical capabilities.

Through its DPI push India is drawing its pathway towards digital sovereignty and technological self-sufficiency and sophistication. One of the biggest influences of Aadhaar has been on Kenya's Digital ID system. Initially, known as Huduma Namba and halted by courts, Kenya has made rapid progress in issuing its new generation digital IDs to citizens – now called the Maisha Namba. Like Aadhaar, Maisha Namba, which is linked to biometrics, will be the primary mode of access to healthcare, education, and other public welfare services. Similarly, Nepal, Bangladesh, Pakistan, and Sri Lanka have in the recent past been implementing their own Aadhaar-like biometric based digital ID systems. In another global push, India has been working with countries around the world to ensure that its digital payments system – UPI is available for select merchants internationally. This includes 7 countries including –

France, Singapore, UAE, Sri Lanka, and Bhutan. Delhi's technological entrepreneurship that is based on open-standards, principles of interoperability, and scalability is attractive to other countries, especially those in the Majority World who wish to exert their digital sovereignty and reject Western digital infrastructure. It helps the Majority World huddle together and challenge long-established Western hegemony on tech governance.

Flexibility and adaptability

It can be argued that shared colonial histories, aligned values, digital self-sufficiency and sovereignty are some of the enabling conditions for the Delhi effect. Regulatory and infrastructural externalization is hinged on these conditions. But another factor enabling the Delhi effect is the flexibility and adaptability of its standards (similar to the Beijing effect). Instead of strict standards resulting in de facto and *de jure* norm externalization, Delhi's regulatory frameworks or its digital infrastructure can be externalized based on a principled transfer. Rules on online content regulation in Pakistan and Sri Lanka might not be copied from Delhi, but share principles of state control. Similarly, Kenya's Maisha Namba or Nepal's national ID might not share the exact same governance frameworks, but can be based on the principles of interoperability and population-wide welfare delivery. This flexibility and adaptability of standards eases the externalization of norms as a corollary to the strict standards of the Brussels effect.

Assessing the desirability of norm externalization

Indian laws governing content-based online platforms and data processing firms offend multiple constitution-backed human rights, including privacy, equality, free speech, and state transparency. They portend a strong trend towards digital authoritarianism with a goal to enhance censorship and state surveillance. India's ranking has been consistently dropping on global indices on free press, freedom on the internet, and the health of democracy.

Similarly, India's adoption and implementation of DPIs is riddled with issues of accessibility, opacity, and concentration of power. India's Aadhaar project continues to battle

challenges of exclusion, security of biometrics, leakage of sensitive data, and exacerbating state surveillance. India's marquee DPI "success" is its digital payments system – the UPI which is a bank-led interoperable payments model that has replaced the duo-ply of Master Card-Visa with a coalition of banks (both public and private) and the federal reserve bank that control access and entry into the system. The two most popular apps that manage 85% of all UPI transactions are owned by US giants – Google and Walmart. India's COVID vaccine rollout was primarily done online, which made it significantly difficult for its disconnected and more vulnerable populations to access life-saving drugs. These systems are not backed by any legislation (apart from Aadhaar and after lengthy court battles) and do not center issues around access, discrimination, and privacy. DPIs are positioned to become Alt-Big-Tech in India. They are often not-based on open-source technology, work in opaque transactions with the private sector, and further a techno-solutionist model of public welfare. As DPIs get exported, especially to other countries in the Majority World, they may exacerbate challenges of exclusion, datafication, and private enrichment. Despite these systemic issues, DPIs remain very popular, their adoption also finding mention as a key goal in the UN Global Digital Compact.

Exporting these trends to other regions in the Majority World would collectively diminish hard-fought digital rights. Overemphasis on the *Brussels Effect* should not blind-side scholars and observers of tech policy from other hidden models of tech governance that may have unforeseen effects on global digital rights.

Future of Global Technology Governance

This article has examined three distinct models of global technology governance influence – the *Brussels Effect*, the *Beijing Effect*, and the *Delhi Effect* – to illustrate the complex mechanisms through which regional powers shape digital futures worldwide. Rather than predicting which regulatory philosophy will ultimately prevail, our analysis reveals that influence in global technology governance extends far beyond formal regulatory externalization and normative value alignments. Each model employs distinctive mechanisms: Europe's unilateral regulatory globalization through market access leverage, China's infrastructure-led pragmatic development approach, and India's hybrid model blending selective adaptation with digital public infrastructure exports. As these models compete and, more importantly, coexist, four critical trends and challenges emerge that may reshape the landscape of global technology governance, particularly for Majority World nations navigating these competing influences.

First, increasing market diversification for digital services globally is weakening the Brussels Effect by reducing the leverage of any single market. Second, economic and institutional constraints within Europe limit its ability to enforce the stringent standards it establishes. Third, while our analysis focuses on norm externalization driven by states, the growing power of private tech firms as governance actors increasingly shapes rules and norms in the global technology space. Finally, shifting geopolitical alignments and the emerging multipolar order fundamentally alter how governance models spread beyond their regions of origin. We examine these trends in turn.

Market Diversification for Digital Services

One of the key conditions for the de facto Brussels Effect is its large and financially wealthier consumer base. This will not change significantly in the near future, but tech companies are getting better at diversifying their

offerings for other large markets in India, China, and Brazil. India is estimated to have one of the largest internet user bases in the world – between 800-900 million (about 55% penetration) just behind China at over a billion (77% penetration). Brazil's internet population stands at about 183 million, at a penetration of 86.2% of the population. With sufficient headroom, these markets offer tech companies great potential to grow their business.

One illustration of market diversification is how WhatsApp (owned by Meta) is making its service interoperable for users in the EU based on requirements in the DMA, but is not extending this feature to some of its largest markets in India and Brazil. Another illustration might be the slow rollout of Apple Intelligence (Apple's consumer AI features) in the EU and China, as compared to other regions to comply with regulations. More stringent rules did not necessarily change global services, but led to service differentiation. Similarly, due to restrictions on processing data placed by the Irish privacy regulator Meta has not launched its AI models in Europe as compared to other regions. In another instance of possible diversification, tech companies might make data available to researchers in the EU to comply with the DSA's research access provisions, but they are unlikely to automatically extend this benefit to other researchers in other countries, especially in the Majority World. The Brussels Effect might remain strong for manufacturing related standards, but diversification (or divisibility of standards) might be easier for tech companies by making changes to their software and internet-based product design to escape the global effects of the strictest standard.

Other conditions that make the *Brussels Effect* strong might be waning too. Strict rules are only as good as their enforcement. Although EU regulators have been imposing large fines, as we have noted, especially on US tech firms, this has not significantly changed either their harmful data-linked business practices or their market dominance, yet. Tech giants, unlike small- and middle-sized enterprises, possess unprecedented financial resources that enable them to absorb regulatory fines. In certain cases companies are also caught misleading regulators or unable to

comply with EU laws, dampening their impact. The European Commission has opened multiple investigations for the non-compliance of the DSA on numerous tech companies. If global corporations, for multiple reasons, can effectively manage non-compliance with European standards, they are unlikely to voluntarily carry them forward to other jurisdictions.

With the political landscape in Europe shifting, its preference for stricter rules might be changing too. This is evident from the numerous speeches and statements made at the recently concluded AI action summit in Paris, where world leaders championed AI innovation instead of centering discourse around AI safety. The EU has also found it challenging to agree on the AI Liability Directive which further illustrates new challenges with institutionalizing strict standards. The EC's President Ursula von der Leyen in her speech at the AI action summit in Paris focused on cutting European red-tape and making Europe a leader in the global AI race. This shift from *AI safety* to *AI innovation* points to a future where the EU may not be the land of the strictest standards, further blunting one of the critical pre-conditions of the Brussels effect.

Economic and Regulatory Constraints

Weak enforcement in Europe also creates doubts, especially among Majority World countries wary of institutionalizing "unenforceable" rules. If the EU with its strict standards and seemingly robust regulatory capacity is finding it hard to rein-in tech firms, Majority World nations who may not have similar economic and regulatory capacities may reject European standards and dampen the de jure Brussels Effect. Instead, as we have shown in the article, they might pursue other alternative models of governance which may work better in their local contexts, economic priorities, and political realities.

Imposing strict standards that require global tech firms to significantly change their business practices and tech-design requires a strong political will and favorable conditions for such tough negotiations. As we have argued, on both conditions, different nations might play their cards to suit

their tech ambitions and a position that promotes technological self-sufficiency and broader geopolitical interests. China's instrumentalization of the GDPR to suit the socio-political and economic agendas present one case. Meanwhile, despite weak privacy obligations, it is not completely unreasonable for the Indian government to adopt favorable data protection standards that do not lead to disinvestments by global tech firms as it actively welcomes foreign investment into its borders. At the same time, India may push WhatsApp to weaken encryption (a demand similar to the EU) or ban multiple Chinese apps for political reasons. It is pertinent to point out that despite court battles and a change in law since 2021, WhatsApp continues to freely offer end-to-end encryption in India to its over 500 million users.

Moreover, the success of the EU's single market builds on market-wide access – companies that comply with EU standards gain entry to its wealthy consumer base. But this might not be true for other countries around the world. If due to dynamic political environments TikTok is banned in India, Senegal, and Somalia, or X in Pakistan and Uganda, tech firms' incentives to carry the de facto Brussels Effect to these countries might be limited. App bans, along with other co-optation of compliance, might push tech firms to subscribe to local cultures to appease political leaders and decision makers, as a more cost-effective way. The culture of app bans is also an influential tactic, once operationalized and normalized, it is easier for other countries to justify and follow. The US' long battle with TikTok to ban the app or shift ownership

The Silicon Valley Effect

The reason tech firms are not deterred by large fines and protracted legal battles, even in Europe, is due to their outsized power. For example, Apple's market capitalization is higher than the GDP of most countries. Zuckerberg, have diminished bargaining power with these firms and their founders. With Amazon, Microsoft, and Google controlling the majority of the critical cloud infrastructure, and Meta and Google managing a significant portion of the ad systems that the internet runs on, the true influence driving tech governance models may lie hidden with these rich

corporations. If essential services like WhatsApp, AWS, or YouTube threaten to abandon countries like India and Brazil due to strict regulation, the position of threat itself will give them an outsized role in negotiations. Millions rely on these services for their livelihood, profession, communication, entertainment, self-expression, and increasingly democratic participation, especially in the Majority World. Governments may not always have the upper hand in policy positions. Due to their market dominance, creating alternatives would be difficult, and maybe in some cases wholly impossible.

Indeed, while the essay focuses on state regulations and other infrastructure related methods as central actors in shaping the rules and norms of the digital future, a key counter-argument is the singular power of tech firms – widely discussed in terms of surveillance capitalism, cloud empires, or the Silicon Valley effect. Essentially, it shows how powerful tech companies engage in regulatory entrepreneurship to establish a transnational legal order that safeguards their global business models. The tech industry's adaptability and global reach further reinforce its ability to shape legal norms beyond traditional state structures, as evidenced by their adaptability to local legal and political norms is their behavior to acquiesce to state demands for content takedowns in India. Despite battles in Australia and Brazil and verbal protests in India, X has removed content related to farmers' protests in India including complete accounts. Recently, YouTube took down a video, on weak justifications, from an online comedy show in India that caused widespread debate on the boundaries of online speech in the country.

A Changing Global Order

The rules of the global order are changing. When the US is cheering domestic businesses and chiding Europe for stringent regulation that stifles innovation, holding tech firms accountable will be an uphill battle and Europe might be disincentivized to play the leading role. At the Munich Security Conference in February, Vice President JD Vance, in a hostile speech, indirectly highlighted that Europe's interests to "regulate" mis- and dis–information is in conflict with US ideals of free

speech. Even Zuckerberg's announcement to loosen the reins on misinformation and harmful content on Meta's online platforms (starting in the US) are clear indications that Europe's strict rules (DSA) might be losing their sheen.

In this new reality, the commitment to the stringent regulatory standards for technology governance will be significantly tested. As the conflict between Ukraine and Russia continues, Europe will also remain dependent on US military support to guard its shared borders with Russia. It remains to be seen whether this reality will impact Europe's hand on tech regulation. China's growing prominence in the "race for AI leadership" already has an impact in changing vocabulary around AI innovation and regulation and will loom large on Western standards of governance, whether in Europe or the US. In a post-pandemic world, where trade negotiations and tariff wars are twisting diplomatic relationships and testing the limits of our globalized world, the Brussels effect is bound to undergo a makeover and create space for other governance models from India, China, Brazil, Australia, and beyond. Tech-policy observers must remain attentive to these global *effects* that may fundamentally reshape digital governance in the coming decades.

Authors

Diyi Liu *is a 2025 Tech Policy Fellow at TGI and holds a DPhil in Information, Communication, and the Social Sciences at the Oxford Internet Institute, University of Oxford.*

Shashank Mohan *is a 2025 Tech Policy Fellow at TGI and currently the Associate Director at the Centre for Communication Governance at National Law University in Delhi.*