Toda
Peace
Institute

REPORT

27 MARCH 2025
REPORT
NO. 216

MAPPING TECH DESIGN REGULATION IN THE GLOBAL SOUTH

Devika Malik

About the Author

DEVIKA MALIK

Devika Malik is a technology policy analyst based in New Delhi working on catalysing effective platform accountability frameworks. She advises tech companies, oversight bodies, think tanks and journalists on platform policy, content risk as well as trust and safety practices. Previously, she led Meta's work on addressing hate speech, misinformation and violent extremism in South Asia. Devika has worked for a decade and a half in legislative research, journalism and with Members of Parliament. She studied Journalism and Conflict Transformation at Lady Shri Ram College, Delhi University and Public Administration at Columbia University.

The views expressed in this report are those of the author(s) alone. They do not necessarily reflect the views of the Toda Peace Institute. An online edition of this and related reports and policy briefs can be downloaded on our website: toda.org/policy-briefs-and-resources.html

Toda Peace Institute
Samon Eleven Bldg. 5F,
3-1 Samon-cho, Shinjuku-ku
Tokyo 160-0017, Japan

Tel. +81-3-3356-5481
Fax. +81-3-3356-5482
Email: contact@toda.org

Abstract

Countries in the Global South exhibit significant diversity in languages, cultures, governments, and economies. A diverse set of incentives across countries in the Global South influences the integration of upstream product and design considerations in digital regulation. This research examines these variations, highlights the state of regulation, and identifies both opportunities and barriers to advancing accountability in digital platforms through design-focused interventions.

Introduction

Governments worldwide are moving to regulate the internet – focussing on governing aspects of data privacy, cybersecurity, competition and intellectual property.

The most far-reaching impacts of social media platforms are felt on civic discourse, manifesting in polarization, extremism, violence, and subversion of democratic processes and institutions. Policy responses to harmful content and its effects on democracy have centered on “content regulation,” which governs compliance and oversight of technology companies on what content is allowable and rules of speech. Content regulation, however, has had limited effectiveness in arresting the harms manifesting from polarizing, hateful, and false narratives online, as these do not address the design choices embedded in tech products that incentivise harmful content that leads to social instability.

Numerous regulations target the digital space, with many aiming to moderate content. However, content moderation is politically contentious, and is widely viewed as censorship. It also requires large teams of people in local languages to make decisions on content that is often traumatizing. Companies are reluctant to invest in content moderation because of the cost.

"Trust and Safety" efforts at large tech platforms often downplay design choices and redirect regulators to focus on content moderation or the removal of harmful content. Many companies claim their platforms are neutral digital public squares, but they are private entities optimizing designs and algorithms for growth metrics tied to advertising profits, compromising privacy, safety, and social cohesion.

Tech insiders and researchers describe many platforms as relying on “anti-social” and deceptive designs that prioritize platform growth and user engagement over user well-being.[1] Social cohesion refers to the factors that hold society together, including civic participation, intergroup relations that uphold human dignity and pluralism, and public trust in institutions. Prosocial technologies can enhance social cohesion by designing features that improve user agency, protect privacy and safety, and enhance understanding in today's complex information environments.

Tech design governance is an alternative, focusing on the design of platforms and the algorithms that determine their content. In the Global North, there are an increasing number of regulatory efforts that recognize the correlation between digital harms and design. For example, the UK and the US state of Minnesota have both passed Age Appropriate Design Codes that require online services that are likely to be accessed by children to design their platforms with children’s best interests in mind, including measures such as providing high privacy settings by default, minimizing data collection, avoiding nudges to weaken privacy,

[1] Monahan, Torin. “Built to Lie: Investigating Technologies of Deception, Surveillance, and Control.” The Information Society 32, no. 4 (2016): 229–240.

and ensuring transparency in how children's data is used. The EU's Digital Services Act (DSA) requires tech companies to give users control for "systemic risks" and calls for user autonomy. While tech companies lobby against such prosocial tech design governance, civil society groups such as the Integrity Institute are influencing the framing of what regulation can and should do as a way of tackling the most consequential harms of social media platforms.

This research reports on desk research and interviews to determine whether there is a similar understanding of how platform design impacts user behaviour in the Global South, and what tech regulations focus on design elements. The report concludes with a set of recommended actions that could bring more context-specific approaches, entry points, and potential champions to design-focused regulation in the Global South.

The Council on Tech and Social Cohesion draws attention to how governments and tech companies might approach tech regulation through contrasting prosocial and antisocial tech designs.[2]

Most of the professionalization of Trust and Safety work has focused on key markets where platform providers have established infrastructure and vital commercial interests, such as the US and EU. Trust and Safety issues, however, are of global importance and are known to disproportionately impact markets outside the US and EU, home to most of the world's internet users. The failure of these systems to contain ethnic and sectarian violence and other societal harms has been documented by civil society and international oversight bodies in Myanmar, the Philippines, India, Sri Lanka, Brazil, Indonesia, and others.

The heterogeneity of languages, social and speech norms, and varying levels of digital literacy compound the challenge of information integrity in the Global South. Product policy and Trust and Safety operations are centralized and Euro-centric. Content moderation at scale in under-resourced languages leads to bias and errors in enforcement; and censorship and human rights violations.

Content governance suffers fundamentally on account of being limited to reactive crisis management and does not address inequitable design choices that platforms are built on.

Content governance also fails in contexts with a democratic deficit. The 'notice and takedown' approach to content moderation is tipped significantly in favour of the State and other hegemonic actors. Transparency disclosures by tech companies themselves repeatedly show the highest numbers of content takedown requests in markets like India. There is also increasing evidence of overreach in executive decision-making and over-compliance with government in these markets, fuelling the risks of digital authoritarianism. Amidst the clamour to reign in Big Tech, India's IT Rules and Data Protection Act, and Sri Lanka's Online Safety Act have all vested greater censorship and surveillance powers with the state. Pakistan's Prevention of Electronic Crimes Act (PECA) has been used to target journalists and rights activists who express dissent against the government.

Content governance suffers fundamentally on account of being limited to reactive crisis management and does not address inequitable design choices that platforms are built on. Biased training data in AI systems disproportionately affect the majority of the world, and the Global South is not prioritized when it comes to ranking and data labelling investments. By virtue of linguistic concentration, marginalized communities are not centred in the product design and safety process. Companies have been unwilling to invest in content moderation systems in non-English languages due to higher costs of labelling and scarcer datasets.

[2] Forthcoming report. Lisa Schirch, et al. Blueprint for Prosocial Tech Design Governance, 2025.

It is in this context that policymaking around platform accountability trains attention on the ways that tech designs steer human behaviours by encouraging, affording, and amplifying certain behaviours. Company and government policymaking can regulate how some platform designs incentivize deceptive and antisocial content and advance the adoption of prosocial design choices. This paper focuses on understanding evolving legal frameworks and governance mechanisms related to digital platforms in non-western contexts. Over the past five years, a significant number of laws, proposed bills and regulations have been enacted or proposed globally, influencing the responsibility of digital platforms, especially social media networks, e-commerce platforms, and intermediary services.

Box 1

Unique Challenges for Tech Governance for the Global South

Countries in the Global South exhibit significant diversity in languages, cultures, governments, and economies. Despite these differences, they face unique challenges in technology governance compared to Western countries due to social, economic, and political factors.

Eurocentric Design Bias: Technology platforms developed in Western countries often prioritize Western norms and values, which can marginalize local contexts and create products ill-suited for the cultural nuances of the Global South. This bias, coupled with the reliance on Western-centric datasets for AI systems, can lead to systemic bias and a lack of transparency in algorithmic decision-making.

Linguistic and Cultural Diversity: The Global South's linguistic diversity poses a significant challenge for large-scale content moderation. Platforms tend to prioritize dominant languages, ignoring the needs of diverse communities due to limited profitability. The expense of data labelling and limited availability of non-English datasets discourage investment in moderation systems for other languages and dialects. This neglect results in biased moderation, endangering freedom of expression and deepening societal divisions. The combination of linguistic diversity, varied social and speech norms, and differing levels of digital literacy in the Global South makes content moderation at scale incredibly difficult. The Global South faces more severe challenges of biased and inaccurate enforcement and instances of censorship and human rights violations.

Economic and Infrastructure Constraints: Limited digital literacy, inadequate infrastructure, and widespread poverty hinder equitable technology adoption and governance in the Global South. This digital divide exacerbates existing inequalities and limits individuals' and communities' participation in the digital economy.

Democratic Deficits and Authoritarian Overreach: In countries with weaker democratic institutions, governments may use technology regulations to suppress dissent, enhance surveillance, and enforce censorship. The "notice and takedown" content moderation method tends to favour state and elite actors.

Research methodology and goals

This study looks into recent regulatory developments in platform governance in six Global South countries: India, Pakistan, Sri Lanka, Brazil, Kenya and Nigeria. The study began with desk research to review the rules enacted and proposed over the last five years relating to platform governance and online safety. These included online safety laws (where applicable), intermediary liability, data privacy, cybersecurity, terrorism, and specific child protection laws.

The goal of this research is to understand the extent to which tech sector related policies in these varied contexts address tech design; including how legal frameworks approach the responsibility of platforms to design products that are safe and compliant with national and international standards and how they are held accountable through compliance and oversight mechanisms. Further, we look at how design governance as an approach to platform accountability could advance in these countries.

A. To understand whether conceptual resonance exists with 'prosocial design' and 'design governance' in the Global South.

B. To look for and learn from innovative proposals/ policy experiments in different areas of online safety and expand the definition/ ‘menu’ of prosocial design governance frameworks to reflect global experiences. The research took a broad view of design governance – i.e., provisions relating to product vs. notice and takedown/oversight/compliance.

C. In keeping with the Council’s goal to catalyze the field of Prosocial Tech Design, explore where the constituencies to seed these ideas might be and how we should thematically and programmatically frame our mission and activities to align with the priorities and capacities of different stakeholders in these jurisdictions.

The research employs a multi-method approach combining desk research, interviews, and regulatory analysis. The methodology is designed to capture a comprehensive view of the current legal landscape and to assess how these laws are being interpreted and implemented in practice.

POLICY MAPPING

The research began with a review and analysis of key rules, regulations, and bills related to platform governance and online safety laws, including intermediary liability frameworks, data privacy and protection laws, cybersecurity laws, and child protection laws. For the mapping, we took a broad definition of tech design governance, distinguishing between regulatory provisions related to **product features** versus content moderation, safe harbour, notice-and-takedown, and oversight frameworks.

STAKEHOLDER ENGAGEMENT

Next, semi-structured interviews were conducted with 25 policy analysts, legal experts, and researchers from the identified countries which identified insights into the practical implications of these regulations, the political and cultural context of platform regulation proposals and their legislative journeys. Interviewees shared how different interest groups, civil society and policymakers perceive the role of design governance in platform regulation (e.g., product design, algorithmic transparency, user safety features).

Gaps in current policy frameworks and ways that laws can be enhanced to better address online safety, platform accountability, and user rights were identified.

CROSS-JURISDICTIONAL COMPARISON

This report seeks to compare and contrast the approaches to platform governance across different jurisdictions. It combines insights from desk research and interviews to offer a comprehensive picture of the state of platform governance. By combining legal analysis with stakeholder perspectives, this research will offer a holistic view of how platform governance laws are evolving and how they can be strengthened to meet the challenges posed by the fast-paced digital environment.

Key findings

Recent regulatory mandates looking at platform governance in most countries have taken the form of privacy/data protection laws and online safety bills that define platform/intermediary liability. In scanning these for design-related provisions, we find that platform design is frequently discussed with respect to a) management of harmful content, b) algorithmic transparency and the right of users to information about automated decision making, and c) data portability and interoperability [3]. These trends are discussed below:

1 DESIGN/PLATFORM-RELATED PROVISIONS AIMED AT ENHANCING MODERATION – PROACTIVE MONITORING OF CSAM, AND TERRORIST CONTENT

India’s IT Rules, 2021, were designed to ensure accountability of intermediaries and platforms for harmful content. The rules developed over a public consultation period of 5 years incorporate some design-related provisions on Proactive Monitoring and Traceability. Platforms are required to deploy automated tools or technology, such as AI, to detect Child Sexual Abuse Material (CSAM), terrorist content, and content inciting violence or hatred. The rules require platforms to remove or disable access to such content proactively, especially before it gains widespread reach.

Significant social media intermediaries (SSMIs) must enable the identification of the first originator of a message or content on their platforms. This impacts platform design, requiring metadata capture mechanisms or reengineering of encrypted systems while adhering to privacy principles.

Similar to India’s IT Rules, Brazil’s Fake News Bill (Brazilian Law on Freedom, Responsibility and Transparency on the Internet) emphasizes traceability and moderation but has a broader focus on transparency. The Bill incorporates several design-related provisions aimed at preventing the virality of disinformation and ensuring transparency in platform operations. Platforms, particularly messaging services like WhatsApp and Telegram, are required to implement mechanisms to trace the origin and dissemination of content that has been forwarded extensively (e.g., forwarded to more than five users or groups); retain metadata for viral content for a specified period to facilitate investigations of disinformation campaigns; and deploy proactive content moderation systems, such as AI-driven tools, to identify and address misinformation and harmful content, including hate speech and CSAM. Visual indicators (e.g., tags like "Forwarded multiple times") must be integrated into the messaging app’s interface. The Bill also envisions integrations with external fact-checking APIs or systems that must be embedded in the platform's architecture. Proactive identification and labelling of misinformation and harmful content is required, with penalties for failing to act promptly.

In Pakistan, the Prevention of Electronic Crimes Act, 2016 (PECA) sets key obligations for platforms to combat harmful online activities, requiring the deployment of moderation systems to address online harassment, child sexual abuse material (CSAM), and hate speech. Complementing this, the Draft Personal Data Protection Bill, 2021 emphasizes Data Protection by Design, mandating that systems minimize data processing risks, particularly for children. Additionally, guidelines for online platforms encourage the integration of tools that enable users to report and block harmful content easily, while also advising platforms to increase transparency in their algorithmic decisions to reduce bias and potential harm.

[3] See Annex 1

2 ALGORITHMIC TRANSPARENCY AND THE RIGHT TO EXPLANATION OF AUTOMATED DECISIONS

Brazil has incorporated algorithmic transparency and data governance through its comprehensive General Data Protection Law (LGPD) and recent moves in AI regulation. Pakistan and Sri Lanka are still in the early stages of formalizing rules around algorithmic transparency. Generally, the concept is closely tied to data protection laws, with rights to explanation, accountability, and audits for high-risk algorithms becoming a common thread. However, challenges in enforcement, lack of comprehensive AI regulation, and the rapid evolution of digital technologies remain significant hurdles across these countries. Platforms are required to disclose how their algorithms prioritize or promote content and any use of automated systems for content curation and moderation.

Platforms must implement tools that allow users to understand why specific content appears in their feeds or is recommended. The framework emphasizes that there should be standards for algorithmic transparency and accountability, with proposals for periodic audits of AI models and algorithms, especially in sectors like healthcare, finance, and education.

Notably, the framework provides for user control over recommendations. Users must have the option to view content in chronological order instead of algorithmically curated feeds. Platforms need to provide easily accessible toggles or settings for users to opt out of recommendation systems.

The Digital India Act, currently under consultation, aims to regulate various aspects of the digital space, including algorithmic governance. While the specifics are still evolving, the draft mentions the need for algorithmic accountability and the responsibility of online platforms to disclose the functioning of algorithms that affect users' experiences. The draft calls for platforms to share information about the functionality and operation of algorithms used to suggest content, make recommendations, or target ads to users.
India's Consumer Protection (E-Commerce) Rules, 2020, introduced by the Ministry of Consumer Affairs, emphasize the need for transparency in automated decision-making processes, especially by online platforms like e-commerce companies. E-commerce platforms must disclose whether the ranking of products or services is influenced by algorithms and, if so, the factors that determine the ranking. Platforms must ensure that automated processes do not lead to unfair treatment of consumers and that users understand how their data is being used.

The Non-Personal Data Governance Framework, published in 2020 by the Ministry of Electronics and Information Technology (MeitY), suggested that data-sharing frameworks should ensure transparency, especially regarding the use of data by algorithms. It acknowledges the need for accountability in how non-personal data is processed and used in AI algorithms.

3 INTEROPERABILITY

Each of these countries is at a different stage of embedding data interoperability into their legal frameworks. While India and Brazil lead with advanced systems and sector-specific implementations, others like Pakistan, Sri Lanka, Kenya, and Nigeria are still developing comprehensive mechanisms to ensure data flows across platforms securely and efficiently. Data portability by design is important because it empowers users to seamlessly transfer their data between services, promoting user autonomy, innovation, and fair competition in the digital economy. With data portability, users can migrate their online networks and content to prosocial platforms. Big tech companies have resisted interoperability, holding users hostage to their platforms. Prosocial tech innovations in the Global South will benefit from interoperability standards which would allow small, local platforms to compete with big tech platforms.

India does not currently have standalone laws on data interoperability, but related provisions are embedded in broader legislative and policy frameworks. The Draft Digital Personal Data Protection Bill, 2022 promotes data portability as a user right, enabling individuals to transfer their personal data between service providers, enhancing interoperability. Additionally, the National Digital Health Mission (NDHM) emphasizes interoperability in healthcare, requiring digital systems to adhere to standardized data exchange protocols for seamless integration across health platforms. Similarly, India's Account Aggregator Framework under the Reserve Bank of India (RBI) facilitates secure and interoperable financial data sharing between banks, financial technology (fintech), and other regulated entities, fostering innovation in financial services.

Pakistan’s legal framework does not directly address data interoperability, but initiatives like the Draft Personal Data Protection Bill 2021 highlight principles that indirectly support it. The bill emphasizes user rights, including data access and portability, which can facilitate interoperable systems. Moreover, the State Bank of Pakistan (SBP) promotes financial data interoperability through the Raast Payment System, a real-time digital payment system that ensures seamless data integration among banks and payment service providers. These measures aim to foster a collaborative ecosystem across financial and digital sectors, although comprehensive interoperability standards are yet to be formalized.

Sri Lanka is still in the early stages of developing data interoperability laws. The Draft Data Protection Act 2022 hints at interoperability by granting individuals the right to data portability, allowing seamless data transfers between systems. Furthermore, the government’s Digital Economy Strategy promotes the creation of interoperable digital infrastructures to enhance public service delivery and foster innovation. Specific interoperability protocols, especially for sectors like healthcare and finance, are under development to align with global standards and encourage cross-platform collaboration.

Brazil has advanced data interoperability laws and frameworks, primarily driven by its General Data Protection Law (LGPD). The LGPD establishes data portability as a fundamental right, requiring organizations to facilitate secure and standardized data transfers between entities upon user request. Additionally, Brazil’s Open Banking Initiative, regulated by the Central Bank, mandates interoperability in financial services by creating standardized APIs for seamless data sharing among banks and fintechs. Similarly, the National Health Data Network (RNDS) ensures interoperability in healthcare by implementing common standards for data exchange among healthcare providers.

Box 2

Global South Tech Regulation Proposals Addressing Design Choices

Innovative prosocial design regulatory proposals are emerging from the Global South, including:

Proactive Monitoring and Traceability: India's IT Rules require platforms to proactively identify and remove harmful content, such as CSAM and terrorist material, potentially necessitating metadata capture or re-engineering encrypted systems to trace the original source. Likewise, Brazil's Fake News Bill requires platforms to trace viral content origins, retain metadata, and implement proactive moderation systems.

Algorithmic Transparency and Right to Explanation: Brazil's LGPD and AI regulations emphasize algorithmic transparency and data governance. Pakistan and Sri Lanka are developing formal rules with a growing focus on transparency, explanation rights, and accountability. India's forthcoming Digital India Act proposes that platforms reveal algorithm functionality, especially for content suggestion and ad targeting. The Consumer Protection (E-Commerce) Rules in India mandate transparency in automated decision-making, requiring disclosure of algorithms used for product ranking and ensuring fairness.

Interoperability: Global South countries are at varying stages of legal integration for data interoperability. Pakistan indirectly supports interoperability through the Draft Personal Data Protection Bill and Raast Payment System. Sri Lanka’s Draft Data Protection Act and Digital Economy Strategy enhance data portability and interoperability. Kenya’s Data Protection Act advocates for interoperable frameworks. Nigeria’s Data Protection Regulation (NDPR) promotes interoperability through user control and data portability. India's Digital Competition Bill fosters digital ecosystem fairness and includes anti-competitive practices like bundling.

Deceptive Design: Global South experts recommend leveraging adjacent sectors like competition and consumer protection to advance prosocial design goals. For example, The Advertising Standards Council of India has published guidelines to address deceptive design patterns. It has partnered with a design research group to promote ethical design and evaluate app design based on a "Conscious Score."

Kenya's Data Protection Act 2019 indirectly supports data interoperability by granting users rights to access and transfer their personal data between service providers. The country's efforts in digital transformation, particularly through the Digital Economy Blueprint, emphasize the need for interoperable systems in areas like e-government, healthcare, and financial services. Initiatives such as the Kenya Health Information System (KHIS) and the Integrated Payment System (IPRS) aim to create interoperable frameworks to enhance service delivery and foster innovation.

Nigeria's Data Protection Regulation (NDPR) 2019 encourages data interoperability by emphasizing user control and data portability, though implementation mechanisms are still evolving. The country's National Digital Economy Policy and Strategy (NDEPS) highlights the importance of interoperable systems to enable efficient public service delivery and foster innovation in digital services. Sector-specific initiatives, such as the Bank Verification Number (BVN) System in finance, demonstrate efforts to create interoperable frameworks, particularly for secure and seamless data exchange within regulated industries.

Barriers in adoption of global standards on prosocial design

1 STRINGENT DESIGN REGULATION CAN BE SEEN AS INHIBITING TECH ADOPTION AND DIGITAL INCLUSION

Global South countries are at varying stages of digitalising their economies and societies; in many cases, states are still focused on developing digital public infrastructure, internet accessibility, and digital literacy while focusing on health tech, educational tech, financial tech, and e-commerce. This reflects the policy priorities of governments and civil society: data privacy, cybersecurity, consumer protection, and now the ethical use of AI. In many Global South contexts, emerging from decades of anaemic growth, militarist or colonial regulatory legacies, there is a general caution against overregulation that could deter investment and hinder the development of beneficial emerging technologies.

Following the UK's adoption of the Age-Appropriate Design Code, similar provisions have been discussed in India and Brazil. Tech companies themselves have advanced these changes in policy discussions as it is expedient for them to comply globally with UK/US standards. However, sections of civil society believe that stringent design guardrails might inhibit the adoption of tech products for online learning/other social uses.

Section 9 of India's Digital Personal Data Protection Act addresses the governance of children's data and children's privacy. The act's approach to regulating children's data is widely discussed as one of the most contentious parts of India's new law. It requires all data fiduciaries (platforms, browsers, OS providers, search engines, etc.) to take 'verifiable parental consent' if they are processing the data of a user below 18 years of age unless they have been deemed 'verifiably safe.' This provision's operationalisation not only requires changes to interface and platform design, but the extent of its application can also have unintended consequences on children's safety, autonomy, and anonymity. The Act provides no guidance on operationalising parental consent. There are strong concerns that age assurance mechanisms may lack efficacy, create inequity in access, lead to privacy concerns, and impose cost barriers and inconveniences in enabling children to engage with online experiences.

Estimates from India's National Statistical Office reveal that, as of 2020-2021, less than 40% of Indians knew how to copy or move files on a computer, with an even lesser proportion having knowledge of internet use.[4]

[4] https://www.livemint.com/news/india/in-charts-which-states-are-the-best-on-computer-literacy-11678468713746.html

The survey also found that digital literacy is better in younger age groups and is reduced among older populations. Further, digital literacy is worse in rural households. The law's reliance on parental consent assumes parents are better placed to understand the potential risks of online data processing. This ignores empirical evidence of the digital divide faced by the elderly, where parents seek advice from their children about navigating digital devices and the internet. In a survey of around six thousand secondary school children conducted by the Delhi Commission for Protection of Child Rights (DCPCR) and the Young Leaders for Active Citizenship (YLAC), over 80% of the respondents said their parents asked for their assistance using digital devices.[5] Stringent Age Verification measures could risk digital exclusion due to demographic and digital realities. In a foreword to this study, the Indian regulator on electronics and IT cautioned against over-standardisation of safety measures and "balancing challenges like the digital divide, shared device usage, low digital literacy, and gender norms around internet access." Other studies point to how age verification technology creates barriers for disabled users and enhances privacy concerns.[6]

2 GEOPOLITICAL AND INFRASTRUCTURAL INTERESTS OF BIG TECH ARE OVER-REPRESENTED IN POLICY DISCUSSIONS

In many countries around the globe, big tech companies provide digital infrastructure for other businesses to promote R&D and innovation. They provide essential market and informational infrastructure, such as Wi-Fi access and cloud services, for consumers, businesses, and government, creating value and dependencies for other players in the market. Big tech companies play a prominent role in the fintech market.

Big tech companies augment state capacity by providing digital infrastructure, specifically by using data for enabling the state to communicate with underserved populations. Last year, Microsoft announced a 14.7 billion Reais investment over three years in Cloud and AI infrastructure and provided AI training at scale to upskill five million people in Brazil.[7] In 2016, Google launched the Google Station project (now defunct) in India to provide free high-speed public Wi-Fi to more than 400 train stations in India. At its peak, in June 2018, more than eight million people used the service every month. Google also announced plans to launch a second cloud region in India to strengthen cloud services for businesses, hospitals, and other public sector organizations.

Tech companies can use their position as both platform providers and platform participants to privilege their own products and services and enter new product markets. Their interests are also often over-represented in policy discourses. Even though data privacy and online safety mandates are focused on maintaining states' sovereignty, viz big tech, few regimes in the Global South possess the geopolitical and institutional clout to actively confront American tech giants on design choices.

In countries like India, traceability regulations (that threaten encryption) are being judicially challenged both by civil society and WhatsApp, while Brazil is struggling to enforce profit-sharing mechanisms with news outlets. However, zero-rating products like Free Basics and TikTok Lite are available mostly across the Global South but violate the principle of Net Neutrality, which requires internet service providers (ISPs) to treat all internet traffic equally. This means that ISPs cannot discriminate based on the user, content, application, or device. Zero-rating apps also have lower privacy and content protections.

[5] https://thequantumhub.com/wp-content/uploads/2023/11/TQH-YLAC-Childrens-Privacy-under-DPDP-Act-2023.pdf
[6] https://www.teenvogue.com/story/age-verification-technology-disabled-people
[7] https://news.microsoft.com/pt-br/microsoft-announces-14-7-billion-reais-investment-over-three-years-in-cloud-and-ai-infrastructure-and-provide-ai-training-at-scale-to-upskill-5-million-people-in-brazil/

3 FRAGMENTED POLICY ECOSYSTEM

Government/Regulators	Civil Society
• Access (Digital Divide • Intermediary/Platform Liability • Data Protection (Data sovereignty, cross-border data flows) • National Security,Terrorism (Traceability,data-flows, terrorist/extremist content) • Competition • Consumer Protection(Dark Patterns) • Cybersecurity (Financial Fraud) • Safety	• Access (internet shutdowns) • Surveillance (data privacy, spyware, encryption) • Censorship • Safety • Language Equity (mostly aimed at improving moderation, sometimes about UX/UI) • Platform economy/ gig workers -Rights and well-being of moderators • Competition (Platform Neutrality, Interoperability, Data portability, algorithmic collusion) • Net Neutrality (Zero-rating, TikTok Lite) • Design Inclusivity • Deceptive Design

Table 1 Conflicting internet governance priorities between the state and civil society

The dichotomy between economic value accruing to emerging economies and the associated social harms is not salient in popular discourse. Civil society in these regions finds itself diminished, with limited constituencies advocating for change. Experts interviewed for this research pointed to how, despite extensive public consultation, several drafts of the Brazilian Fake News Bill over four years suffered on account of aggressive lobbying by Big Tech companies and lack of consensus among stakeholders. Some interviewees perceived the provisions on systemic risk measurement and "duty of care" as a way to soften intermediary liability, i.e., legal liability of platforms for harms occurring due to third-party content. Civil society ultimately withdrew support from drafts sponsored by Big Tech and right-leaning senators due to fear of private censorship. Misinformation, polarization, and hate speech remain strategic tools in electoral politics, creating a strong political interest in keeping content moderation minimal/narrowly focused on dissent.

On the flip side, some sections of civil society see engagement-based ranking as having benefited rights activists, independent political candidates, and independent journalists, especially in contexts where legacy media is appropriated by the state and its affiliates. Engagement-based ranking can be seen as amplifying independent voices and supporting social causes.

4 REGULATORY CAPACITY

Regulatory capacity is a key consideration. Most interviewees were sceptical of regulators in their jurisdiction on account of competence to effectively oversee complex tech design and independence. Regulation remains a double-edged sword in contexts with a democratic deficit[8]. The clamour for tech regulation has resulted in regulatory overreach that spills over to hamper civic space. For example, Sri Lanka recently introduced the Online Safety Bill (2023), designed to combat online harm, particularly cyber harassment, hate speech, and misinformation. The bill proposes establishing a National Online Safety Commission tasked with overseeing content moderation, investigating complaints, and ensuring compliance with safety standards. However, critics argue that the bill could enable censorship and stifle free expression, particularly in politically sensitive contexts.

Competing interests among different agencies can result in inconsistent regulations. Nigeria's Draft Code of Practice for Interactive Computer Service Platforms/Internet Intermediaries was introduced by the National Information Technology Development Agency (NITDA) in June 2022. It outlines obligations for online platforms and intermediaries to ensure user safety, transparency, and accountability. However, concerns over its potential misuse and enforcement challenges remain key issues for stakeholders. Experts argued that the Code as subsidiary or secondary legislation will remain ineffective and limited in operation. They also questioned the suitability of the Ministry of Communications over the Ministry of ICT in bringing such a law.

5 INFORMATION AND KNOWLEDGE ASYMMETRIES

There's often a significant gap in knowledge about how digital platforms are built and function. This limits stakeholders' awareness of the correlation between digital harms and upstream design features and inhibits their ability to engage effectively in discussions about design regulation. Major tech companies keep critical information about their algorithms and data practices proprietary, which can prevent local developers from innovating or adapting technologies to local contexts.

Many researchers in India noted that Government funding to civil society is decreasing and almost all research is funded by tech companies, contributing to ecosystem capture. For example, Brazil's Draft Bill went ahead of most other legislative proposals in modelling the EU Digital Services Act's provisions regarding data access to researchers. However, researchers interviewed noted the local research ecosystem was not equipped to handle public APIs, and a lack of safeguards could lead to executive overreach.

Recommendations and opportunities

1 CO-CREATE POLICY AND DESIGN CODES

The definition of prosocial tech design remains elastic. It merits exploring additional prosocial design principles, including language equity, inclusive design, encryption, access, interoperability, platform and network neutrality, OSINT and decentralization in collaboration with local researchers to expand and develop additional design principles.

More experiments and evidence are needed to build robust theories of change around how design governance can solve issues of language and design equity. Afsaneh Rigot, a researcher at ARTICLE 19 focusing on the Middle East and North African (MENA) human rights issues, has developed the 'Design from the Margins' framework. The method proposes that instead of retrofitting tech design for marginalised ('decentred') groups, the most vulnerable communities of users should be proactively identified and designed for at the outset. This design should then be generalized for the remaining user base. [9]

[8] https://scholarship.law.georgetown.edu/facpub/2548/

[9] Rigot, Afsaneh . “Design From the Margins.” May 13, 2022

2 STRATEGIC ALIGNMENT WITH COUNTRY CONTEXTS, ADJACENT SECTORS

Even where legislative intent does not centre on social cohesion or safety, prosocial outcomes can inadvertently come from aligning with strategic priorities. Looking at adjacent sectors like Competition, Antitrust, and Consumer Protection regulations could surface innovative avenues to discuss tech design.

For example, in India, the discussion about interoperability has gained ground in the context of fostering digital competition. The proposed Digital Competition Bill emphasizes interoperability as a key measure to ensure fairness in the digital ecosystem. Design innovation tends to follow closely behind the strategic and regulatory focus. The Beckn Protocol developed in India, is an open, decentralized, interoperable protocol designed to eliminate gatekeepers from digital commerce. A critical use case of the protocol has been the Open Mobility Initiative, where any mode of transport can contribute to providing services to commuters, eliminating the dependency on any third parties. Also in India, the Namma-Yatri App (auto/tuk tuk-hailing app) built on the protocol logged 10 million rides within a year of its inception.

The Digital Competition Bill aims to reduce market barriers by mandating dominant digital platforms to adopt standardized protocols that promote compatibility with other platforms. The Bill also takes a firm stance against anti-competitive practices such as tying and bundling, where dominant platforms force users to adopt one service to access another. Deceptive design has also been framed in the discussions on the Bill as a challenge to competition.

The Advertising Standards Council of India (ASCI) has published self-regulatory guidelines for Online Deceptive Design Patterns in Advertising to address the issue of deceptive design patterns (Dark Patterns) prevalent in online advertising. In addition to identifying 12 deceptive design practices frequently used by e-commerce apps, it has partnered with a local design research group to launch an 'Ethical Design Library' to promote 'conscious design' and also helps evaluate app-design with a 'Conscious Score'.

3 ECOSYSTEM DEVELOPMENT, AWARENESS AND NARRATIVE-BUILDING

It is important to take an ecosystem-level view of activities to encourage the tech design governance agenda while looking at policy as a second or third-order outcome. A more immediate effort is needed to inform the discourse on tech design policy and algorithmic decision-making while catalysing the tech and research communities. This could entail collaborating with journalists, educators and creators from the Global South to create multimedia resources aimed at demystifying platform design and operations and their impacts on society. For example, Alaphia Lab in Brazil, The Big Tech Narrative Initiative andRightsCon through its short-story showcase on Big Tech surveillance, are some examples of efforts to encourage innovative storytelling around tech and society.

This research was sponsored by the Council on Technology and Social Cohesion.

ANNEX

For a full version of this table, including the legislative language, please click here.

Parameters	Interventions	Regulatory Approach
Tech-enhanced moderation	Proactive Content Moderation	Rule 3(1)(b) of Information Technology (Intermediary Guidelines and Digital Media Ethics) Rules 2021 (India), and Article 12 of the Law on Freedom, Responsibility and Transparency in the Internet 2020 (Brazil)
	Tracing the first originator of the message	Rule 4(2) of the Information Technology (Intermediary Guidelines and Digital Media Ethics) Rules 2021 (India), and Article 10 of the Law on Freedom, Responsibility and Transparency in the Internet 2020 (Brazil)
	Retaining metadata for viral content	Article 11 of the Law on Freedom, Responsibility and Transparency in the Internet 2020 (Brazil)
	Disabling authorization by default	Article 9 (IV) of the Law on Freedom, Responsibility and Transparency in the Internet 2020 (Brazil)
	Minimising data processing risk	Section 8.2 of the Personal Data Protection Bill 2021 (Pakistan)
Algorithmic Transparency	Right to explanation	Article 10 (§2) of General Data Protection Law, (Brazil) and Digital India Act (India)
	Accountability (disclosure of functioning of algorithms)	Article 20 (§1) of General Data Protection Law (Brazil), Digital India Act (India), and Rule 5(3)(d) of the India Consumer (E-Commerce) Rules 2020 (India)
	Users' control over recommendations	Article 20 of the General Data Protection Law (Brazil)
Interoperability	Data portability	Digital Personal Data Protection Act (2023) (India), Section 10.2 of the Personal Data Protection Bill (Pakistan), Data Protection Act (Sri Lanka), Article 11(§4)(I) of the General Data Protection Law (Brazil), Section 38(2) of the Data Protection Act of 2019 (Kenya), and Part 3, Regulation 3.1(15) of the Data Protection Regulation 2019 (Nigeria)
	Interoperable financial services or digital infrastructure	Account Aggregator Framework (India), Raast Payment System (Pakistan), Digital Economy Strategy (Sri Lanka), Digital Economy Blueprint (Kenya), Health Information System (Kenya), and National Digital Economy Policy and Strategy (NDEPS) (Nigeria)

THE TODA PEACE INSTITUTE

The Toda Peace Institute is an independent, nonpartisan institute committed to advancing a more just and peaceful world through policy-oriented peace research and practice. The Institute commissions evidence-based research, convenes multi-track and multi-disciplinary problem-solving workshops and seminars, and promotes dialogue across ethnic, cultural, religious and political divides. It catalyses practical, policy-oriented conversations between theoretical experts, practitioners, policymakers and civil society leaders in order to discern innovative and creative solutions to the major problems confronting the world in the twenty-first century (see www.toda.org for more information).

CONTACT US

Toda Peace Institute
Samon Eleven Bldg. 5 th Floor
3-1 Samon-cho, Shinjuku-ku, Tokyo 160-0017, Japan

Email
contact@toda.org

Sign up for the Toda Peace Institute mailing list
https://toda.org/policy-briefs-and-resources/email-newsletter.html

Connect with us on the following media.
YouTube: @todapeaceinstitute3917
X (Twitter): https://twitter.com/TodaInstitute
Facebook: https://www.facebook.com/TodaInstitute