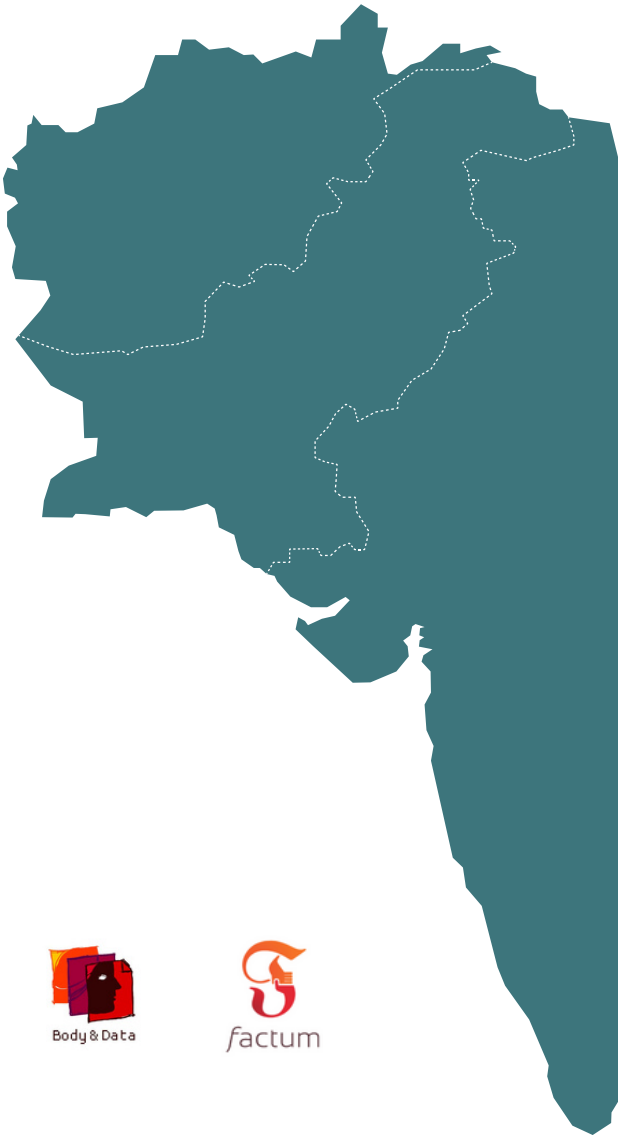
February 2025

WHITEPAPER

Digital Governance and Rights in South Asia, and the Path Forward



TECHGLOBAL INSTITUTE

blast ব্লাস্ট

BOLO BHI
Advocacy - Policy - Research

Body & Data

factum

TABLE OF CONTENTS

Acknowledgment

This paper has been drafted by Faisal Lalani, with final refinements by Shumaila H. Shahani.

Last year, 12 digital rights organizations across South Asia came together in Kathmandu to exchange lessons and learnings amid rising state-sanctioned and platform-mediated technology authoritarianism in the region. The discussions tackled a broad range of issues, from repressive digital laws and policies to whether or not existing models of platform accountability are working in South Asia, to the impact of geopolitics on domestic technology ecosystems. This whitepaper is an outcome of the conversations which have taken place over the past year, with an aim of developing a South Asia-focused digital rights network that collaborates and exchanges best practices in addressing the sprawling and interconnected issues of technology governance and accountability across a range of technologies from digital public infrastructure to platforms in one of the fastest growing regions in the world.

We are grateful to numerous civil society organizations, individuals and activists who provided invaluable feedback in shaping this paper. We are additionally grateful for contributions from Farieha Aziz, Dovan Rai, Omar Rajaratnam, Saritha Irugalbandara, Sabhanaz Rashid Diya, and Shahzeb Mahmood.

Executive Summary

This white paper explores the digital rights challenges in South Asia, particularly in the context of emerging technologies and the influence of frameworks from Global North on regional technology policy. It examines how global governance standards intersect with the socio-political realities of the Global South, where civil society faces dual pressures: state overreach and the imposition of external regulatory agendas. The paper argues that South Asia's digital rights landscape is shaped by a series of tensions and structural misalignments that not only put vulnerable populations at risk but also undermine effective governance.

A key issue discussed is the widening gap between international regulations and the political realities of South Asian states. International regulatory models often disregard the institutional capacities of local governments, resulting in policies that are either overly ambitious or unenforceable. Years of state control over digital spaces have exacerbated the erosion of trust between governments and civil society, making it increasingly difficult for digital rights regulations to gain legitimacy. This widening trust deficit underscores the need for tech policies that are context-specific, locally informed, and responsive to the region's unique socio-political challenges. Effective digital rights policies must also foster greater accountability and collaboration between governments and civil society actors. When global frameworks are imposed without consideration of local complexities, they risk exacerbating governance challenges rather than resolving them. Addressing these issues requires embedding technology governance within existing institutional frameworks.

In response to these challenges, the paper proposes a series of policy recommendations, emphasizing the importance of civil society engagement, adaptive governance frameworks, and the strengthening of local accountability mechanisms. To ensure these efforts extend beyond national borders and have a broader impact, there is an urgent need for a South Asian digital rights coalition. Such a coalition would facilitate regional collaboration, enabling civil society to collectively advocate for a more equitable, locally relevant approach to digital rights. Given the increasing use of emerging technologies to suppress dissent and consolidate state power, this coalition is not just necessary but urgent. Cross-border cooperation would empower South Asian countries to assert their own governance priorities, strengthen protections for digital freedoms, and build resilience against

both state and transnational threats to digital rights.

Introduction

Currently, 46% of the population of South Asia is connected to the mobile internet and over 80% now have access to a 4G or 5G smartphone (GMSA, 2024). The proliferation of digital technologies has led to at least 35 tech-centered regulations, over 20,000 court cases against human rights violations (Reporters Without Borders, 2024), and around 170 internet shutdowns between South and Southeast Asia (Access Now, 2024).

Several countries in South Asia, including Bangladesh, India, Nepal, Pakistan, and Sri Lanka, have been experiencing a decline in fundamental rights such as privacy and freedom of expression. Governments in the region have long exploited state machinery to frame their oppressive governance as necessary for national security, economic prosperity, and geopolitical autonomy. With the emergence of new technologies, politically and economically unstable institutions have become even more effective tools for expanding state control. These trends stem from the ongoing erosion of civic freedoms, driven by the manipulation of religious, ethnic, caste, and gender divisions, and their conflation through overt nationalism. The decline in rights has been further intensified by disinformation campaigns, targeted censorship, and covert surveillance, while weakened institutional protections have left little room for collective action.

Technology companies inevitably become complicit. Although the vast majority of their users reside outside this region, these firms are predominantly domiciled in the Global North (Tworek, 2021). This historical underinvestment means a lack of resources for content moderation in local languages, weak accountability and enforceability mechanisms, and a widening trust gap between public and private sectors. Compliance efforts are often superficial, as companies have little incentive to establish meaningful safeguards—their headquarters remain in the Global North, and public discourse there rarely prioritizes issues affecting the Global Majority. Countries in regions like South Asia must continually negotiate the trade-offs between sovereignty, governance, and equitable access to technology.

In response to these pressing challenges, digital rights-focused civil society organizations (CSOs) have

emerged as key advocates. These groups engage in specialized interventions through either legislation, litigation, public investigation, transparency efforts, and/or user empowerment to promote accountability and digital freedoms (Tech Global Institute, 2024). While each approach is multifaceted and offers contextualized frameworks of accountability, CSOs continue to face systemic resistance, insufficient funding, gaps in technical knowledge, and are often denied a seat at the table during the decision-making processes. Beyond these organizational struggles, a more fundamental issue looms over digital governance: the absence of a collective movement for digital rights.

One major barrier to mobilization is the illusion that technological progress is inevitable and beyond public influence, leading to passive acceptance of surveillance capitalism. Opportunities to drive change in this field are often monopolized by the Global North, restricting participation to an exclusive exchange among a privileged few. The resulting initiatives attempt to challenge deeply entrenched economic structures but remain disconnected from real-world contexts. The outcome is a perilous fragmentation driven by righteous indignation yet lacking practical direction. Any meaningful framework for change risks being buried in technical jargon or legal limbo, seldom transcending symbolic gestures or repetitive appeals. The digital rights movement across the region benefits from broad participation by technologists, academics, lawyers, journalists, and social scientists. What it currently lacks—and urgently needs—are organizers who can bridge gaps between sectors and unify the movement. The necessary ingredients for a mass movement are already in place: momentum across sectors is at an all-time high, public scrutiny of tech companies is pervasive, and governments, across political lines, largely agree on the need for regulatory safeguards. Despite such favorable conditions, there is no unified direction.

The idea of cohesion is not novel: since the conception of South Asia as a regional force in the original South Asian Association for Regional Cooperation (SAARC) convening, similar initiatives have sprung up over time: the South Asia Regional Energy Partnership (SAREP) ensured regional access to reliable energy; the Southasia Peace Action Network (Sapan) pushes for a visa-free, unified partnership in the region; and even smaller, bidirectional alliances have formed between South Asian nations to establish economic cooperation and trade agreements, resource and knowledge sharing, and joint security efforts. But as of yet, there is no formal agreement among South Asian nations to address digital rights. This is particularly concerning given the region's significant engagement with

content takedown and user data requests to digital intermediaries.

At the same time, South Asia faces a significant lack of investment from major tech companies—a challenge common to many Global Majority countries—while CSOs continue to face systemic obstacles and deliberate efforts to undermine their work.

This lack of regional cooperation has led to a contagion effect, where emerging markets in South Asia are implicitly compelled to adopt governance frameworks and regulations set by dominant markets, primarily in Australia, Canada, the European Union (EU), and the United States. This alignment is often appealing to both private and public stakeholders, as it promotes global standardization, facilitates intergovernmental oversight, and enhances the attractiveness of local markets for foreign investment and expansion. The most notable example of this phenomenon is the Brussels Effect—the EU's ability to shape global markets through its own regulatory policies (Bradford, 2020). Given the EU's economic influence, companies operating within its jurisdiction must comply with its standards, adjusting their production, manufacturing, and deployment practices accordingly. To minimize costs and avoid the complexity of designing specialized products for different markets, businesses often opt to apply EU standards uniformly across their entire global product output. Foreign investors with significant stakes in EU markets are incentivized to align with its regulations, and policymakers in other countries frequently adopt EU standards as a model for their own governance frameworks. A key example of this is the *General Data Protection Regulation* (GDPR), which has become one of the most influential global benchmarks for data protection, shaping regulatory approaches in countries such as Bangladesh, India, Pakistan, and Sri Lanka. Similar patterns can be observed elsewhere, such as the Washington Effect, which has influenced policies on platform accountability and content moderation. These theories of geopolitical and economic influence assume a standardized approach to governance, overlooking the sociocultural particularities of individual contexts and opting out of these global regulatory frameworks carries significant risks, including potential withdrawal of funding from intergovernmental organizations that support civil society and public initiatives.

These global contagion effects are also evident in more localized settings. India, for instance, exemplifies what might be termed the Delhi Effect—a regional spillover influenced by shared legal traditions among former British colonies where its digital priorities shape the technology policies of neighboring

South Asian countries. It is particularly noticeable in India's export of its digital public infrastructure (DPI), a deeply integrated technological ecosystem widely embedded in the daily lives of Indian citizens holding immense economic value. India has strategically leveraged DPI as a form of soft power, promoting its adoption in other countries through its interoperability, user-centric design, and ease of deployment (Parveen, 2024). As a result, Bangladesh, Sri Lanka, Nepal, and the Maldives have integrated elements of India's DPI, while other Global Majority nations have drawn inspiration from initiatives like Aadhaar and the Unified Payments Interface (UPI). The Delhi Effect also extends to technology policy, with India's *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021* and *Digital Personal Data Protection Act, 2023* setting legislative precedents and influencing regulatory approaches in its neighboring countries (Mahmood, 2022).

The combined impact of these regional and global contagion effects—along with fragmented accountability mechanisms, systemic discrimination, and the weakening of civil society—has led to a highly inconsistent digital rights landscape across South Asia. Each country now faces its own set of challenges, grappling with digital governance issues that lack coordinated oversight.

Bangladesh

Bangladesh's journey in tech regulation has developed significantly over recent decades. In the early 2000s, the country recognized the need to support the growth of Information and Communication Technology (ICT) as a means of fostering economic progress. The foundation for technological regulation was laid with the introduction of the *Bangladesh Telecommunication Regulation Act, 2001* and the *National Information and Communication Technology Policy, 2002*. Subsequently, the *Information and Communication Technology Act, 2006* was enacted by the Bangladeshi Parliament under the government led by the Bangladesh Nationalist Party. Thereafter, over the next fifteen years, the Awami League government's digitization efforts significantly transformed Bangladesh, including facilitating internet access to over half of the country's population. This expansion accelerated the growth of the country's technology sector and led to the establishment of a nationwide biometric national identity system. This rapid expansion of digital technology occurred alongside strongman policies that strengthened the Awami League's control over

personal data flows and online content. By leveraging operating licenses as a means of influence, the government granted itself broad powers, including the ability to shut down or throttle internet access, remove online content arbitrarily, and penalize human rights defenders, activists, and journalists for content deemed "anti-government" (Diya, 2024). In the absence of institutional checks and balances and with weak technological infrastructure, data governance became largely synonymous to state control with oversight responsibilities haphazardly distributed, and significant barriers to non-state actors' ability to hold authorities accountable. Public dissent is severely restricted due to limited legal challenges against judicial overreach, uncertainty over which regulatory body holds responsibility, and a general lack of access to information for civil society. More broadly, the framing of rights as human rights versus constitutional rights does little to safeguard freedoms, as economic and political priorities routinely take precedence over human rights concerns.

TABLE 1 - RELEVANT TECH-RELATED POLICIES IN BANGLADESH

Law	Description
Bangladesh Telecommunication Regulation Act, 2001	• Established a commission (BTRC) to regulate telecommunication and internet service providers. • Criminalizes various expressions, allows blocking and monitoring of communications. • Grants the Ministry of Home Affairs and intelligence authorities authority to collect user data for national security, public order, and other vague grounds.
Information and Communication Technology Act, 2006	• Aimed at securing online content and electronic data. • Allowed government interception powers for national security, sovereignty, public order, and foreign affairs. • Granted state authorities broad and arbitrary authority under now repealed section 57 to curtail free speech, with similar concerns continuing under later laws.
Pornography Control Act, 2012	• Criminalizes possession, distribution, production, and use of pornography, including child pornography and content likely to arouse sexual desire.

	• Does not regulate deepfake pornography or provide measures to remove or stop distribution of content deemed illegal under the law.
Digital Security Act, 2018	• Enacted to address cybercrime, digital threats, and protect online information. • Criminalized spreading "false information" and "digital espionage." • Broad language restricted speech creating potential for misuse and arbitrary enforcement.
[Draft] Regulations for Digital and Social Media Platforms 2021	• Introduces intermediary liability on digital, social media, and over-the-top (OTT) platforms, requiring local registration, content moderation, and a complaints system. • Expand BTRC's authority for content removal. • Risk restricting access to information and communication and limiting freedom of expression.
[Draft] Over the Top Content Based Service Provision and Management Policy, 2022	• Proposes banning OTT platforms from offering news, talk shows, and current affairs, and restricting broad categories of prohibited content. • Requires platforms to categorize content by age and establish mechanisms for handling complaints. • Mandates OTT platform registration with the Information Ministry and grants BTRC authority to block or remove prohibited content.
Cyber Security Act, 2023	• Repeals the *Digital Security Act 2018* but retains most of its offenses, continuing to restrict free speech. • Like its predecessors, it contains broadly defined offenses that enable subjective interpretation, facilitating censorship, arbitrary arrests, and vexatious legal actions.
[Proposed] Personal Data Protection Bill, 2024	• Removes the localization requirement for sensitive and user-generated data but retains it for undefined categories of "classified data" without any procedural safeguards (Shiekh, 2024). • Allows personal and non-personal data to be transferred for inter-state trade, international relations, or as determined by the government (Islam, 2023).

	• Affords exemptions to state actors, including law enforcement and intelligence agencies, from compliance requirements.
[Draft] Bangladesh Telecommunication Regulation (Amendment) Bill, 2024	• Aims to replace older telecommunications laws, expanding platform regulations through higher fines for non-compliance, oversight of mergers and acquisitions, and the creation of a regulatory sandbox (Hasan, 2024).

India

From the onset of the 21st century, India's tech regulatory framework has been primarily focused on achieving digital sovereignty, with an emphasis on control over data, autonomy, and security (Lalani, 2024). Governance in this domain has largely been shaped by executive actions rather than legislative oversight. Though often framed as progressive, a closer examination reveals significant concerns about the concentration of state power and the erosion of individual privacy.

The fragmented nature of India's digital governance is evident in the multiplicity of regulations, each addressing a distinct aspect of the digital ecosystem. The *Digital Personal Data Protection Act, 2023* sets a baseline for data privacy but also grants the government extensive authority to control data flows and enforce data localization, which raises concerns about the potential for state surveillance (Burman, 2023). Similarly, the *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021* and the *Broadcasting Services (Regulation) Bill, 2024* contain provisions aimed at content moderation, positioning the government as the central arbiter of online speech (Singh, 2022). The *Digital India Act, 2023* introduces a focus on online safety, particularly with regard to algorithmic transparency and AI risk assessments (Sheikh, 2024).

Each new regulation revises and reframes concepts from earlier laws while consistently maintaining vague language. Although often defended as necessary for adapting to emerging technologies, this ambiguity serves as a tool to shield the government from accountability. Instead of introducing concrete safeguards, these laws frequently postpone meaningful oversight to future legislative revisions. The DPDPA, for example, was

significantly diluted over its years-long development, leaving broad exemptions for government entities and lacking clear restrictions on surveillance and data processing without consent (Panjiar, 2023). The Intermediary Guidelines introduce a traceability provision that compels platforms to identify the original sender of messages—undermining end-to-end encryption and severely compromising user security (Bansal, 2021).

TABLE 2 - RELEVANT TECH-RELATED POLICIES IN INDIA

Law	Description
Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021	• Threatens privacy and freedom of expression, enables censorship, and facilitates unlawful government surveillance.
[Proposed] Digital India Bill, 2023	• Aims to replace the *Information Technology Act, 2000*, addressing digital governance, online safety, intermediary accountability, and emerging technology risks. • Despite pushback from tech companies, it has received overwhelming support (Shiekh, 2024).
Telecommunication Act, 2023	• Repeals the *Telegraph Act, 1885* and *Wireless Telegraph Act, 1933*, granting broad government powers to intercept messages, break encryption, and impose internet shutdowns. • Creates a communications surveillance framework that forces platforms to disclose user content in an intelligible format, inconsistent with necessity and proportionality principles.
Digital Personal Data Protection Act, 2023	• Developed over six years, the statute introduces vague data processing rules, government-appointed oversight, and exemptions for data fiduciaries. • Lacks data portability and the right to be forgotten, reduces private sector compliance burdens, and introduces broad government blocking powers. • Raises concerns over definitional ambiguity, blanket exemptions, and mandated data localization.

[Proposed] Broadcasting Services (Regulation) Bill, 2024	• Aims to create regulatory uniformity across traditional broadcasting and digital streaming services, requiring licenses and establishing content evaluation committees. • Concerns include unclear implementation, over-compliance risks, and potential censorship.
[Proposed] Digital Competition Bill, 2024	• Inspired by the EU's *Digital Market Act*, the statute introduces an ex-post intervention framework, where the Competition Commission acts after anti-competitive conduct occurs.
[Proposed] Digital Personal Data Protection Rules, 2025	• Fails to clarify vague terminology such as "national security" or "public interest" within the *Digital Personal Data Protection Act, 2023*. • Raises concerns about broad discretionary powers for government agencies.

Nepal

Having held its first election as a republic in 2017, Nepal has struggled to keep pace with the evolving challenges of the digital age. In its early stages, its tech policy ecosystem is characterized by low internet penetration, inadequate telecommunications infrastructure, and a stark digital equity gap (Lamichhane, 2022). As a result, the country lags behind the rest of the region in recognizing digital rights and integrating digital inclusion.

A particularly critical gap in Nepal's digital governance is its inadequate legal recognition of online harms. Critical issues such as gender-based violence, disinformation, hate speech, and cybercrime continue to be governed by outdated legislation, most notably the *Electronic Transactions Act of 2008* (EngageMedia, 2023). Compensation mechanisms remain antiquated. Instead of assessing harm based on its gravity and context, the current framework categorizes offenses by the medium in which they take place, placing greater emphasis on offline harms. Consequently, acts of digital violence often receive disproportionately lower penalties and reparations compared to similar offenses committed offline. This reliance on obsolete laws has reinforced inequities, as their broad provisions, lack of specificity, and technical shortcomings impede effective enforcement and meaningful accountability.

More recently, the government has embraced a form of tech-driven nationalism, promoting state-led digital

initiatives as a pathway to modernization. This is most apparent in its cybersecurity measures and the introduction of a biometric national identity card for its citizens. The proposed cybersecurity framework includes a government-controlled internet gateway, which would centralize online traffic under state supervision, enabling authorities to censor and surveil content deemed offensive or inappropriate (Castor, 2023). Meanwhile, the biometric identification system seeks to expand digital access to essential services but has faced criticism for disproportionately impacting vulnerable populations and serious concerns about data privacy and potential misuse (Opiah, 2024).

These developments highlight a broader pattern in Nepal's digital policies, where state control and surveillance take precedence over user rights and digital inclusivity. Furthermore, the limited presence of civil society in digital rights advocacy has made it difficult to establish public accountability measures or grassroots efforts for reform.

TABLE 3 - RELEVANT TECH-RELATED POLICIES IN NEPAL

Law	Description
Electronic Transactions Act, 2008	• Sought to ensure security and authorization in electronic transactions and address cybercrimes like piracy, source code alteration, confidentiality breaches, and fraud. • Criminalizes vaguely defined acts related to "illegal materials" and "harmonious relationships." • Has been misused to detain journalists and rights activists, and suppress online criticism of the government.
National Cyber Security Policy, 2023	• Proposes a government-controlled internet and telecom gateway, inspired by China's Great Firewall and Cambodia's National Internet Gateway. • Criticized for enabling surveillance and censorship, potentially fragmenting the internet and restricting free data flow.
Directives for Managing the Use of Social Networks, 2023	• Regulates social media use while promoting self-regulation among users and platforms on manipulated media, obscene content, unauthorized sharing, and deceptive calls. • Criticized for targeting criticism and social media activities, while lacking clarity on issues like fake pages and accounts.

	• Resulted in Nepal banning TikTok over hate speech concerns, later lifted after the platform complied with government-mandated content regulations.
Social Media Bill, 2025	• Criminalizes fake and anonymous profiles, false information, and deepfakes. • Requires data localization and content moderation and proposes strict penalties. • Grants excessive powers to the government to criminalize dissent and increase surveillance.

Pakistan

Through increasing trends of prosecuting free flow of speech and categorizing anti-military and government content as blasphemous (Sohail & Durrani, 2023), Pakistan has adopted a techno-authoritarian approach to the internet. From heightened surveillance powers being granted to its intelligence agencies (Asad, 2024) to banning platforms for hosting "objectionable content," the country fails to provide judicial grounding or transparency in its actions of filtering, blocking, and taking down content (Jahangir, 2024). Its courts continue to approach new digital media regulations with an antiquated media mindset, failing to account for the complexities of modern digital communication.

These oppressive practices have been codified primarily through the *Prevention of Electronic Crimes Act (PECA), 2016* and the influence of the *Pakistan Telecommunications Authority* (PTA) (Ahmed et. al, 2023). Initially introduced as a legal framework to address digital harms, PECA is laden with vague provisions that grant authorities broad enforcement discretion. Rather than serving its intended purpose, the law now facilitates government overreach under the guise of national security (Aziz, 2022). Empowered by PECA, the PTA frequently restricts internet access as a means of suppressing political dissent, while internet shutdowns have become a routine tool for silencing religious or political opposition (Migliano, 2025). Recent amendments have further expanded PECA's reach, introducing stricter provisions that legitimize and extend military surveillance powers (Amnesty International, 2025).

These developments coincide with increased internet restrictions since 2024. VPN disruptions, initially attributed to a "technical glitch," were later justified under a new VPN

registration mandate issued by the PTA under the *Monitoring and Reconciliation of Telephony Traffic Regulation, 2010* (Ali, 2024). Officials defended the measure as necessary to curb "immoral" content and terrorist activity. Simultaneously, users experienced slow internet speeds, allegedly due to web-management system upgrades, raising concerns about a national firewall following previous deployments of Sandvine technology (Aziz, 2024). Government officials have provided conflicting statements on the existence of such a system, but patterns of throttling, slow speeds, and VPN restrictions indicate enhanced digital surveillance without official disclosure. Furthermore, under PTA directives, telecommunication companies operate a mass surveillance system, as confirmed by an Islamabad High Court ruling that exposed warrantless data interception (Abbas, 2024). This was later reinforced by a government notification authorizing the country's intelligence agency to conduct surveillance for "national security."

Litigation has emerged as the primary avenue for civil society to hold the government accountable. Alongside this, CSOs actively engage in policy advocacy, public awareness efforts, and capacity-building programs while also providing legal assistance in digital rights-centered court cases.

TABLE 4 - RELEVANT TECH-RELATED POLICIES IN PAKISTAN

Law	Description
Prevention of Electronic Crimes Act, 2016	• Has been used to charge journalists, political activists, and academics for "anti-state" and "anti-institution" speech. • Criminal defamation has been abused against women in retaliation to #MeToo disclosures. Constitutionality challenged before courts and currently pending decision by the Supreme Court. • Various High Courts have called out the investigation agency for abuse of power. • A presidential ordinance expanded its scope to include the institutions of military and judiciary as potential targets of cyber offenses, thereby increasing digital policing.

Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules, 2021	• Grant PTA unconstitutional censorship powers. • Challenged before the Islamabad High Court, which directed revisions, no changes implemented as of yet. • The government has been blocking social networking sites citing non-compliance with the rules and takedown requests.
[Proposed] Personal Data Protection Bill, 2023	• Despite discussions since 2005, no formal data protection law has been enacted. • Existing draft mandates data localization, requiring critical personal data to be stored in Pakistan. • Proposed data protection regulator under federal government control. • Uses ambiguous terms such as "national security," "legitimate interest," and "public interest."
Punjab Defamation Act, 2024	• Hastily passed with jurisdiction extending beyond the province. • Allows public officeholders to be claimants and shifts burden of proof to defendants; claimants do not need to prove loss or damage. • Cases are heard by government-appointed tribunals with powers to impose fines and disable social media accounts. • Defendants do not have the right to a defense by default; they must request permission to present one. • Remains under challenge before the Lahore High Court.
Prevention of Electronic Crimes (Amendment) Act, 2025	• Further tightens the government's control over the digital landscape. • Introduces offenses such as false and fake information with vague and ambiguous framing throughout.

Sri Lanka

Sri Lanka's ongoing challenges with digital rights are largely rooted in the government's consistent violations of freedom of expression. Legal frameworks such as the *International Covenant on Civil and Political Rights (ICCPR) Act of 2007* have been used to justify the ethno-religious targeting of

individuals, including the imprisonment of entertainers, while the *Prevention of Terrorism (Temporary Provisions) Act of 1979* grants the state broad and unchecked authority to act against perceived threats (Freedom House, 2024). These laws reflect a broader institutional pattern of consolidating political power under the guise of national security, enabling state overreach without adequate oversight.

Despite being the first South Asian country to enact a privacy law—the *Personal Data Protection Act of 2022* (Nahra et al., 2022)—efforts to promote a more balanced regulatory approach have faced obstacles. Civil society groups initially attempted to introduce a self-regulatory *Code of Practice for Online Safety* sought to ensure more robust content moderation and compliance standards on online platforms developed through public consultation and the involvement of diverse stakeholders (Lalani & Irugalbandara, 2024). However, after communication and diplomacy with technology firms fell short, the government insisted on pushing forth the *Online Safety Act, 2024* instead, which continues the pattern of enacting abusive legislations. The statute has vague terminology, lacks clear contextual definitions, and places interpretative power in the hands of executive bodies with contentious agendas.

At its core, Sri Lanka's struggle with digital rights is tied to deeper structural issues, including economic instability, public distrust in the government, and systemic failures in addressing gender-based violence and other forms of discrimination. While the country has a strong and active civil society, perspectives on digital rights remain fragmented, with mobilization occurring primarily in response to pressing threats rather than through sustained advocacy.

TABLE 5 - RELEVANT TECH-RELATED POLICIES IN SRI LANKA

Law	Description
Personal Data Protection Act, 2022	• Sri Lanka became the first South Asian country to pass a data protection law, modeled after the EU's GDPR, targeting all businesses that process data within Sri Lanka and related to its citizens. • Ensures data is accurate, transparent, accessible, and provides right to erasure.
Online Safety Act, 2024	• Contains vague terms like "national security threats" and "distress" with no legal precedent or context.

	• Enforcement left to the regulator, composed solely of executive-appointed individuals. • Enables takedown of online content critical of the government. • Enacted without considering the Sri Lanka Code of Practice for Online Safety and Responsible Content developed by industry association.

Thematic Overlaps

Each country examined in this report walks a tightrope, where pushing back against the state carries significant risks, and civil society opposition remains muted. Funding from international donors is often attached to objectives far removed from the lived realities of local communities. Challenges of adopting global governance frameworks are a common denominator across the region, particularly around the cost management of compliance with international regulations, the dichotomy between consumer-oriented versus rights-oriented laws, and the insistence of states to adopt the latest and greatest tech policy when political institutions are ill-equipped to support them, remains persistent. Moreover, domestic tech policies are heavily influenced by occidental standards, resulting in a form of elite capture where the priorities of the Global North dictate the regulatory direction of South Asia.

This dynamic enables the exploitation of existing discriminatory fault lines in ways not always apparent in the original legal frameworks. For instance, fundamental rights such as freedom of expression—often assumed in the Global North—remain underdeveloped in many South Asian countries. Consequently, imposing digital governance models without first addressing such offline structural issues risks deepening existing power imbalances.

Against this backdrop, five key themes emerge as prevalent challenges across South Asian countries. Based on a survey of twelve digital rights organizations representing the in-focus countries, a visual assessment maps the positioning of each country along two axes: institutional maturity (i.e., the extent to which each issue is embedded within legal, political, and economic frameworks), and structural resilience (i.e., the capacity of civil society and the public to resist and advocate against these challenges).

Techno-Nationalism

A political ideology that ties a country's technological advancement to its geopolitical standing (Capri, 2019), techno-nationalism emerged as a central theme. In South Asia, political elites increasingly equate national strength with technological capabilities, whether through the development of DPI, investment in AI research, or dominance in hardware manufacturing and supply chains. Justifications based on national security, resistance to influence from the Global North, and concerns over foreign intervention have further reinforced this ideology, blending ambitions for economic and technological growth with mechanisms of state control. This perspective has become deeply embedded in state policy, influencing how governments regulate and promote technological innovation. As a result, governments strive for digital sovereignty, using technology governance to mold online ecosystems in ways that align with political priorities. This concentration of control not only limits digital freedoms but also extends state influence into traditionally protected offline spaces.

Vague and Oppressive Laws

Governments merge aspirations for technological growth with mechanisms of state control, creating a flexible legal framework that can be shaped to serve political interests. This dynamic is reflected in the institutions responsible for drafting and enforcing regulations, which are often led by authoritarian figures whose priorities lean more toward political agendas than toward equitable digital governance.

As a result, a wave of legislation has emerged, marked by inconsistencies, abstract rhetoric, and remnants of colonial legal frameworks. Key terms like "national security" and "public interest" are frequently left undefined, allowing regulatory bodies, typically composed of government-appointed officials, to interpret these concepts as they see fit. This broad discretionary power enables the selective enforcement of laws, which reinforces state control while undermining efforts to create a balanced and just digital environment.

While justifications have traditionally centered around national security concerns, governments are increasingly invoking human rights issues—such as protecting women and children from online harm, combating hate speech, and addressing disinformation—as pretexts for expanding surveillance and restricting digital freedoms. Although these concerns are legitimate, their instrumentalization allows for vague, overreaching regulations that disproportionately target political dissidents, journalists, and CSOs. Consequently, such laws serve as a tool of state control rather than protection.

Executive Overreach

In a deliberate effort to consolidate the central government's absolute authority, executive overreach is a common feature across many countries. Regulatory bodies established and empowered under primary and secondary legislation are often placed directly under the influence of the executive branch, which has the power to control their composition and set their agendas. This concentration of power allows governments to bypass judicial oversight, enabling executive bodies to exercise disproportionate control over digital ecosystems with minimal accountability. As a result, measures like mass surveillance, platform shutdowns, and algorithmic policing are implemented with little to no transparency.

Identity-Based Disenfranchisement

Identity-based disenfranchisement has emerged as one of the most alarming consequences of the growing consolidation of state power in the digital realm. Marginalized communities, including ethnic and religious minorities, political dissidents, and gender-diverse populations, are systematically excluded through digital mechanisms often presented as neutral or progressive. For instance, biased digital identification systems can limit access to essential services for certain groups, while algorithmic discrimination in law enforcement disproportionately targets people due to flawed data. As a result, digital access has evolved beyond a mere issue of technological connectivity; it has become a matter of fundamental rights and civic participation, as exclusion from digital systems undermines individuals' ability to fully engage in society.

Civil Society Co-Opting

The efficacy of CSOs was another prevalent theme. Several factors determine the strength of a country's civil society landscape, including financial stability, technical expertise, and strategic coordination with other CSOs. However, many CSOs operate under significant constraints, including restrictive funding environments, dependency on third-party resources, and external political pressures. U.S. funding cuts, for example, have severely weakened digital rights advocacy by reducing financial support for grassroots initiatives. Reliance on foreign donors with conflicting interests further forces CSOs into procedural engagement rather than substantive advocacy, as funding conditions often prioritize diplomatic and geopolitical interests rather than local advocacy needs. These limitations create a compliance-driven civil society landscape, where CSOs struggle to mount meaningful resistance against state overreach. As a result, rather than acting as an effective counterbalance to government control, CSOs often find themselves constrained within frameworks that reinforce, rather than challenge, oppressive digital policies.

Ultimately, the cumulative effect of these themes results in a digital landscape shaped not by inclusivity and innovation but by exclusion, coercion, and centralized power.

Policy Considerations

Given the wide variety of political, economic, and cultural nuances that exist even within South Asia, it is imperative to have policies that are contextualized to the themes and patterns addressed above. The logic behind these policies must be informed by the perspective of users from each of these countries, instead of imposed frameworks borrowed from the Global North. Specifically, new policies should consider the following:

Addressing the erosion of trust:
As evidenced repeatedly in the overreaching, power-hoarding tech policies being passed in each country, there is a long history of distrust between civil society and the institutions which govern them. Yet, Western-centric models of global governance rarely, if at all, account for this critical power imbalance. Instead, they often assume a level of institutional accountability that does not exist in many contexts. New policies must account for the risk of state exploitation as carefully as they do for private sector exploitation.

Technology as a relative construction:
A common misconception is that technological challenges can be addressed through isolated policy interventions or by introducing new technologies as quick fixes. It is imperative to understand that technology is embedded within the fabric of historical, political, and institutional structures that have gone through their fair share of scrutiny and reform. Effective digital policy must therefore move beyond treating technology as an unprecedented phenomenon. Instead, frameworks should be grounded in local legal precedents and governance experiences, learning from past successes and failures to create policies that are both contextually relevant and structurally sound.

Deeper engagement with civil society:
Though consultations with lawyers, journalists, technologists, and activists are often promised and claimed to have been carried out, these always fall short due to personal and political resistance to incorporating dissenting views, or a lack of technical expertise among stakeholders at the table. Effective governance requires an ongoing, structured relationship between policymakers and CSOs that study the implications of emerging technologies in real time. However, engagement must be a two-way process—civil society must also ensure that its advocacy is cohesive, accessible, and actionable for policymakers to translate into stronger, rights-driven legislation.

Adaptive and dynamic framework:
As technology rapidly evolves, regulations must be equally responsive to emerging innovations and their societal impacts. Rigid, static policies

risk becoming obsolete or ineffective in addressing new challenges. However, this does not mean laws should be loosely framed. Instead, governments should establish a structured evaluation process, conducting periodic reviews to assess the effectiveness of laws, regulations, and policies. This approach helps identify gaps, mitigate unintended consequences, and refine governance strategies, ensuring that digital regulations remain both forward-looking and adaptable.

In exploring alternative digital rights interventions that incorporate these principles, we highlight three proven local approaches to accountability.

Judicial activism serves as a crucial check on state overreach, scrutinizing excessive government control and shaping policies through legal precedents. In *Anuradha Bhasin v. Union of India*, the court assessed the legality of internet shutdown orders under various domestic laws, emphasizing that government-imposed restrictions on internet access must be temporary, limited, lawful, necessary, and proportionate (Mahmood, 2023). Currently, Indian courts are assessing the legality of the traceability provision in the *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*, which has been challenged by WhatsApp and its parent company, Meta. This provision would require platforms to weaken encryption, effectively enabling state surveillance.

In Pakistan, multiple legal challenges against expanding digital restrictions remain pending before the courts. The Supreme Court of Pakistan is currently hearing an appeal concerning a provision widely criticized for enabling state censorship. Additionally, high courts are handling cases on social media regulations, the ban on X (formerly Twitter), internet disruptions, unauthorized surveillance, and the implementation of a national firewall. However, judicial independence in Pakistan is steadily eroding, with a recent constitutional amendment marking a significant shift (International Commission of Jurists, 2024). This amendment introduced an extraordinary level of political influence over the judicial appointment process, which threatens to undermine the judiciary's impartiality and its ability to effectively check state overreach.

Thus, while judicial activism can serve as a powerful tool against state overreach, its effectiveness is not absolute. Courts operate within political constraints and are shaped by broader institutional dynamics. A judiciary that lacks independence may fail to function as a meaningful check on executive authority. Nevertheless, even under such constraints, the judicial process remains a crucial avenue for contesting digital restrictions, offering a platform for legal

resistance and setting important precedents, even if its effectiveness is increasingly curtailed by political interference.

Self-regulatory mechanisms led by CSOs is another promising approach. In Sri Lanka, for instance, a network of CSOs has developed a community of practice that fosters accountability by coordinating joint messaging across conferences, panels, and public forums. This ensures a united stance against misaligned donor agendas and state-imposed restrictions while promoting equal representation across cultures and demographics. Digital rights violations affect populations differently within and across countries, making such networks vital for localized advocacy. This model need not be confined to South Asia—many Global Majority countries face similar challenges, including eroding trust in governments, limited engagement with tech companies, and restrictive regulatory environments. A stronger coalition, grounded in regional realities, could reduce reliance on Western-driven agendas and enable civil society actors to push for digital rights on their own terms.

Several mechanisms within the network can further empower civil society. These could include an advisory body composed of subject-matter experts skilled in navigating funding mechanisms, engaging with Big Tech public policy directors, maneuvering through economic crises, recruiting private sector allies beyond the tech industry, organizing legal petitions, or drafting self-regulatory accountability frameworks. Additionally, the network could provide an avenue to coordinate international pressure on country-specific digital rights violations, as well as a collaborative platform for civil society actors to strategize against common challenges, share knowledge, and push back against digital authoritarianism.

Each of these approaches has been effective but remains largely confined within national borders. To amplify their impact, a regional coalition is necessary—one where civil society can collaboratively tackle digital rights challenges. While alliance-building itself is not novel, a structured South Asia-specific coalition focused on tech policy is. The following key tenets would be essential for such an initiative:

1. **Transparency:** A fundamental goal of this coalition may be to enhance transparency in digital governance. Many critical decisions affecting digital rights—such as those made by internet service providers, telecommunication operators, and intergovernmental organizations—remain opaque to CSOs. The coalition should work toward gaining greater visibility into

these financial and operational structures.

2. **Knowledge-sharing:** A key factor in holding powerful institutions accountable is ensuring that CSOs have the necessary information and tools to do so. The coalition may focus on demystifying digital policy, making it more accessible to activists, researchers, and legal experts. This includes breaking down complex regulatory frameworks, sharing best practices from successful digital rights interventions, and providing case studies that highlight both effective strategies and lessons learned from past failures.

3. **Collective Ownership:** A successful coalition cannot function as a centralized body dominated by a single entity. Instead, it must be structured in a way that allows all participating organizations to have a voice and a stake in decision-making. This could be achieved through a rotational secretariat, ensuring leadership is shared among different organizations over time; an oversight committee made up of experts from diverse fields, including law, technology, journalism, and activism; a bi-directional feedback mechanism, where all members contribute to shaping policies, projects, and joint statements; and a decentralized hosting model, where in-person meetings are organized in different member countries to ensure regional representation.

4. **Context-Specific Operations:** To truly represent the region, the coalition must be built around the realities of South Asia. This means scheduling meetings in time zones more appropriate to South Asia, using culturally relevant terminology rather than Western-centric legal and policy language, adopting communication platforms familiar to local stakeholders, and ensuring that branding, messaging, and outreach strategies are informed by South Asian history and culture.

5. **Funding:** One of the key challenges for South Asian civil society is its dependence on donors whose Western-driven agendas often fail to align with local realities. While some funders support regional digital rights work, recent funding issues highlight the need for sustainability. The coalition should map out viable funding sources while prioritizing long-term independence through diversified revenue models. Reducing reliance on external donors ensures greater stability and autonomy in advocacy efforts.

Conclusion

The urgency for a social movement advocating digital rights has never been greater, as emerging technologies are increasingly weaponized to suppress dissent, target marginalized communities, and consolidate power. Efforts to challenge public and private actors responsible for these harms are undermined by limited technical expertise, scarce resources, and the restricted mobility and influence of CSOs. South Asia exemplifies this dilemma, with nearly every country in the region grappling with tech companies that invest minimally in content moderation while state governments exploit this inaction to tighten their grip on power. Attempts at accountability tend to fall short as they are, often by necessity, attached to the whims of intergovernmental organizations and non-regional influence, or swiftly stamped out by the oppressive arms of their central governments.

References

Aaj News. (2024). New internet regulations in Pakistan. https://english.aaj.tv/news/30348914

Abbas, Z. (2024). The surveillance system keeping tabs on millions. Dawn. https://www.dawn.com/news/1843299

Access Now. (2024). Partial enforcement of India's Telecom Act — a total eclipse of digital rights. https://www.accessnow.org/press-release/india-telecom-act-2023-enforcement/

Access Now. (2024). The most violent year: internet shutdowns in 2023. https://www.accessnow.org/wp-content/uploads/2024/05/2023-KIO-Report.pdf

Agarwal, S. & Heda, S. (2023). Media Regulations in India: Government Overreach Disguised as 'Parity'. Tech Policy Press. https://www.techpolicy.press/media-regulations-in-india-government-overreach-disguised-as-parity/

Ahmed S. Z., Yilmaz, I, Akbarzadeh, S., & Bashirov, G. (2023). Digital Authoritarianism and Activism for Digital Rights in Pakistan - ECPS. ECPS. https://www.populismstudies.org/digital-authoritarianism-and-activism-for-digital-rights-in-pakistan/

Al Jazeera. (2024, November 26). Pakistan tests China-like digital firewall to tighten online surveillance. https://www.aljazeera.com/news/2024/11/26/pakistan-tests-china-like-digital-firewall-to-tighten-online-surveillance

Ali, K. (2024). PTA speaks on 'technical glitch', insists on VPN registration. Dawn. https://www.dawn.com/news/1871781/pta-speaks-on-technical-glitch-insists-on-vpn-registration

Ali, K. (2024). Unregistered VPNs won't work after Nov 30, says PTA chief. Dawn. https://www.dawn.com/news/1873356

Ali, K., & Ali, U. (2024). Interior Ministry demands VPNs blockage, claims it is used by 'terrorists to facilitate violent activities.' Dawn. https://www.dawn.com/news/1872561

Amnesty International. (2024). Bangladesh: Interim Government must restore freedom of expression in Bangladesh and repeal Cyber Security Act.

https://www.amnesty.org/en/latest/news/2024/08/bangladesh-interim-government-must-restore-freedom-of-expression-in-bangladesh-and-repeal-cyber-security-act/

Amnesty International. (2025). Pakistan: Authorities pass bill with sweeping controls on social media.
https://www.amnesty.org/en/latest/news/2025/01/pakistan-authorities-pass-bill-with-sweeping-controls-on-social-media/

Article 19. (2016). Bangladesh: Information Communication Technology Act.
https://www.article19.org/data/files/medialibrary/38365/Bangladesh-ICT-Law-Analysis.pdf

Aziz, F. (2024). Project PECA I: How to silence a nation. Prism.
https://www.dawn.com/news/1725805

Aziz, F. (2024). Surveillance central. Dawn.
https://www.dawn.com/news/1845889/surveillance-central

Aziz, F. (2024). The ministry of (dis)information and the ban on X. Dawn.
https://www.dawn.com/news/1828972/the-ministry-of-disinformation-and-the-ban-on-x

Aziz, F. (2024). The privacy myth. Dawn. https://www.dawn.com/news/1844158

Bansal, V. (2021). WhatsApp's fight with India has global implications. WIRED.
https://www.wired.com/story/whatsapp-india-traceability-encryption/

Baral, L. R. (1985). SARC, but no "shark": South Asian Regional Cooperation in perspective. Pacific Affairs, 58(3), 411. https://doi.org/10.2307/2759238

Biyani, N., De Guzman, N. F., Maheshwari, N., & Mahmood, S. (2021). Bangladesh: Regulation for Digital, Social Media and OTT Platforms, 2021. In Internet Impact Brief. internetsociety.org.
https://www.internetsociety.org/wp-content/uploads/2022/03/IIB-Bangladesh.pdf

Bolo Bhi. (2020). Pakistan's online censorship regime.
https://bolobhi.org/wp-content/uploads/2020/07/Pakistan%E2%80%99s-Online-Censorship-Regime.pdf

Bradford, A. (2020) The European Union in a globalised world: the "Brussels effect" - Groupe d'études géopolitiques. Groupe D'études Géopolitiques.
https://geopolitique.eu/en/articles/the-european-union-in-a-globalised-world-the-brussels-effect/

Burman, A. (2023). Understanding India's new data protection law. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en

Calderaro, A., & Blumfelde, S. (2022). Artificial intelligence and EU security: the false promise of digital sovereignty. European Security, 31(3), 415–434. https://doi.org/10.1080/09662839.2022.2101885

Capri, A. (2019). Techno-Nationalism: what is it and how will it change global commerce? Forbes. https://www.forbes.com/sites/alexcapri/2019/12/20/techno-nationalism-what-is-it-and-how-will-it-change-global-commerce/?sh=6765528c710f

Caster, M. (2023). Nepal must revise its cybersecurity policy to avoid further internet fragmentation. Tech Policy Press. https://www.techpolicy.press/nepal-must-revise-its-cybersecurity-policy-to-avoid-further-internet-fragmentation/

Coda Story. (n.d.). Pakistan's nationwide web monitoring program raises alarm. https://www.codastory.com/authoritarian-tech/surveillance/pakistan-nationwide-web-monitoring/

Committee to Protect Journalists. (2024, June). Pakistan province enacts harsh defamation law; Supreme Court presses legal action against 34 media outlets. https://cpj.org/2024/06/pakistan-province-enacts-harsh-defamation-law-supreme-court-presses-legal-action-against-34-media-outlets/

deBoer, F. (2023). How elites ate the social justice movement. Simon and Schuster.

Digital Rights Foundation. (2020). Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules, 2020: Legal Analysis. https://digitalrightsfoundation.pk/wp-content/uploads/2020/12/Removal-and-Blocking-of-Unlawful-Online-Content-Procedure-Oversight-and-Safeguards-Rules-2020_-Legal-Analysis.pdf

Digital Rights Foundation. (2023). Analysis: Personal Data Protection Bill 2023. https://digitalrightsfoundation.pk/wp-content/uploads/2023/07/Legal-Analysis-Statement-on-PDPB-July-2023.pdf

Diya, S. R. (2024). How Bangladesh fell into an information blackout. Tech Policy Press. https://www.techpolicy.press/how-bangladesh-fell-into-an-information-blackout/

EngageMedia. (2023). Digital Rights in Nepal: An Overview. EngageMedia. https://engagemedia.org/2023/gif-digital-rights-nepal/

Ewe, K. (2023). Nepal bans TikTok and tightens control over all social media platforms. TIME. https://time.com/6334769/nepal-tiktok-ban-social-media-regulation/

Fact Focus. (n.d.). Human rights in Pakistan. https://factfocus.com/humanrights/3784/

Freedom House. (2024). Under Siege: Sri Lanka's civic space and the battle for free speech. https://freedomhouse.org/article/under-siege-sri-lankas-civic-space-and-battle-free-speech

Freeman, J. (2013). The tyranny of structurelessness. Women's Studies Quarterly, 41(3–4), 231–246. https://doi.org/10.1353/wsq.2013.0072

Geo News. (2024). Bandwidth bandits: Internet regulation riddle strikes VPNs in Pakistan. https://www.geo.tv/latest/557762-bandwidth-bandits-internet-regulation-riddle-strikes-vpns-in-pakistan

Ghimire, R. (2023). New social media directive in Nepal lacks clarity. OnlineKhabar English News. https://english.onlinekhabar.com/social-media-directive-nepal.html

GSMA. (2024). The state of mobile internet connectivity report 2024. https://www.gsma.com/r/wp-content/uploads/2024/10/The-State-of-Mobile-Internet-Connectivity-Report-2024.pdf

Hasan, M. (2024). Govt drafts fresh telecom act. The Daily Star. https://www.thedailystar.net/business/economy/news/govt-drafts-fresh-telecom-act-3574146

Human Rights Watch. (2022) Pakistan: Repeal Amendment to draconian Cyber Law. https://www.hrw.org/news/2022/02/28/pakistan-repeal-amendment-draconian-cyber-law

ICJ. (2024). Pakistan: 26th Constitutional amendment is a blow to the independence of the judiciary. https://www.icj.org/pakistan-26th-constitutional-amendment-is-a-blow-to-the-independence-of-the-judiciary/

Imperial Law Associates. (n.d.). Highlights of Electronic Transactions Act, 2006 (2063). https://www.lawimperial.com/highlights-of-electronic-transactions-act-2006/#:~:text=T

he%20Electronic%20Transactions%20Act%202063,such%20records%20through%20illegal%20manner.

Islam, M. T. (2023). Protection of privacy in Bangladesh: issues, challenges and way forward. The International Journal of Human Rights, 28(1), 89–124. https://doi.org/10.1080/13642987.2023.2234296

Jacob, H. (2024). The end of South Asia. Foreign Affairs. https://www.foreignaffairs.com/south-asia/end-south-asia

Jahangir, R. (2024). Pakistan on verge of Techno-Authoritarian turn. Tech Policy Press. https://www.techpolicy.press/pakistan-on-verge-of-techno-authoritarian-turn/

Lalani, F. M. (2024) Predicting the direction of digital sovereignty in Post-Election India. New America. https://www.newamerica.org/planetary-politics/blog/predicting-the-direction-of-digital-sovereignty-in-post-election-india/

Lalani, F. M., & Irugalbandara, S. (2024). The Sri Lanka Model: The impact of civil advocacy on tech Policy. Tech Policy Press. https://www.techpolicy.press/the-sri-lanka-model-the-impact-of-civil-advocacy-on-tech-policy/

Lamichhane, R. (2022). Digital inclusion and digital equity. The Kathmandu Post. https://kathmandupost.com/columns/2022/08/28/digital-inclusion-and-digital-equity

Mahmood, S. (2023). Internet shutdowns in Bangladesh: Legal dimensions and recourses. Prepare Prevent Resist. https://preparepreventresist.org/2024/01/17/internet-shutdowns-in-bangladesh-legal-dimensions-and-recourses/

Malik, A, M. (2024). 'Glitch' blamed for VPN disruption. Dawn. https://www.dawn.com/news/1871583

Migliano, S. (2025). Government Internet Shutdowns Cost $7.69 Billion in 2024. Top10VPN. https://www.top10vpn.com/research/cost-of-internet-shutdowns/

Momand, A. (2024). SC suspends IHC order in audio leaks case, bars court from further proceedings. Dawn. https://www.dawn.com/news/1853303

Nahra, K. J., Pinto, T. Y., & Jessani, A. A. (2022). Sri Lanka becomes the first South Asian country to pass comprehensive privacy legislation. WilmerHale. https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-la

w/20220330-sri-lanka-becomes-the-first-south-asian-country-to-pass-comprehensive-privacy-legislation

Opiah, A. (2024). Nepal reverses mandatory national ID requirement for social security benefits. Biometric Update | Biometrics News, Companies and Explainers. https://www.biometricupdate.com/202407/nepal-reverses-mandatory-national-id-requirement-for-social-security-benefits

Panjiar, T & Waghre, P. (2023). DPDPB, 2023 in the Parliament: Dialogue, drama, and discord. Internet Freedom Foundation. https://internetfreedom.in/dpdpb-2023-in-the-parliament/

Parveen, N. (2024). India's DPI: Orchestrating a Digital Transformation. https://www.indiabusinesstrade.in/blogs/indias-dpi-orchestrating-a-digital-transformation/#:~:text=India's%20digital%20public%20infrastructure%20is,leading%20technology%20export%20going%20forward.

Polanyi, K. (1944). The Great Transformation. http://ci.nii.ac.jp/ncid/BA07821290

Qadar, R. G. (2024). PM okays Peca law tweaks to regulate social media. The News International. https://www.thenews.com.pk/print/1186788-why-no-decision-on-may-9-cases-so-far-ask-govt

Reporters Without Borders. (2024). 2023 World Press Freedom Index – journalism under political pressure. ReliefWeb. https://reliefweb.int/report/world/2023-world-press-freedom-index-journalism-under-political-pressure-enru

Riaz, A. (2021). How Bangladesh's Digital Security Act is creating a culture of fear. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2021/12/how-bangladeshs-digital-security-act-is-creating-a-culture-of-fear?lang=en¢er=global

Sheikh, A. (2024). Transparency Must be a Cornerstone of the Digital India Act. Tech Policy Press. https://www.techpolicy.press/transparency-must-be-a-cornerstone-of-the-digital-india-act/

Sheikh, T. M. (2024). Data Localisation and Data Protection in Bangladesh: A review. The Daily Star.

https://www.thedailystar.net/law-our-rights/news/data-localisation-and-data-protection-bangladesh-review-3528661

Singh, A. (2023). India's IT Rules & New Amendments: 'A Threat to Freedom of Expression.' Tech Policy Press. https://www.techpolicy.press/indias-it-rules-new-amendments-a-threat-to-freedom-of-expression/

Sohail, M. & Durrani R. (2023). Digital Rights in Pakistan: A Review of 2023. Digital Rights Foundation. https://digitalrightsfoundation.pk/wp-content/uploads/2023/07/Digital-Rights-in-Pakistan_-A-Review-of-2023-1.pdf

Tech Global Institute. (2024). A New Digital Frontier: A Blueprint for Reforms towards Rights-Respecting Information and Technology Laws in Bangladesh. https://techglobalinstitute.com/wp-content/uploads/2024/12/Whitepaper-A-New-Digital-Frontier-Bangladesh.pdf

Tech Global Institute. (2024). Reimagining 'Tech accountability' in the global majority. https://techglobalinstitute.com/research/reimagining-tech-accountability-in-the-global-majority/

Tworek, H. (2021). Facebook's America-centrism is now plain for all to see. Centre for International Governance Innovation. https://www.cigionline.org/articles/facebooks-america-centrism-is-now-plain-for-all-to-see

Mahmood, S. (2022). Bangladesh: New online content regulation, localisation rules threaten privacy. https://www.context.news/digital-rights/opinion/how-bangladeshs-new-online-content-regulation-threatens-privacy