GNI Submission on the Strategic Priorities of the UN Special Rapporteur on Freedom of Opinion and Expression

1. Strategic Priorities

The thematic framework presented above is intended as a preliminary basis for discussion.

- Looking at this preliminary strategic framework, do you consider it to adequately reflect the most significant challenges and opportunities affecting freedom of opinion and expression today and over the next three years?

In particular:

- Are there important issues, trends, or developments that are not sufficiently reflected?
- Are there thematic areas that should receive greater emphasis or on the contrary, have already received adequate attention?
- Are there other cross-cutting issues that should be integrated across all thematic areas?

The Global Network Initiative (GNI) congratulates Special Rapporteur Leopoldo Maldonado Gutiérrez on his appointment and appreciates the opportunity to contribute to the mandate's priorities. GNI is a multistakeholder organization bringing together more than 130 members, including academics, civil society organizations, investors, and technology companies, to advance freedom of expression and privacy in the technology sector. Over its 18-year history, GNI has worked closely with a range of UN offices, processes, and special mandate holders to advocate rights-based expectations for responsible conduct by governments and the private sector, consistent with international human rights law and the UN Guiding Principles on Business and Human Rights. GNI sees the Special Rapporteur's work as particularly important at a time when governments are expanding the range of laws and policies that address cybercrime, online safety, and artificial intelligence, often with significant implications for how people communicate, access information, and form opinions.

GNI considers the preliminary framework a sound basis for the mandate's work. Drawing on members' experience and our work on government policies and company practices affecting freedom of expression and privacy, we encourage the Special Rapporteur to give particular

attention, over the next three years, to two connected priorities: (i) the expansion of government powers over data and communications, addressed through three distinct areas as set out below, and (ii) growing challenges to transparent, inclusive, and accountable digital policymaking, addressed further in Section 3 of this submission.

Cross-border data sharing and digital transnational repression

Personal data and communications are increasingly affected by overlapping regulatory frameworks. Laws developed to address cybercrime, cross-border evidence-sharing, data localization, online safety, age assurance, and AI can each create new obligations to collect, disclose, retain, or process personal information. Without adequate safeguards, they can expose users to surveillance, restrict access to information, and be misused beyond their stated purpose. Even where these laws are carefully drafted and implemented, their overlapping requirements and processes can lead to unintended impacts on freedom of expression, especially when affected individuals are unwilling or unable to effectuate their rights. GNI encourages the Special Rapporteur to examine, together with other Special Mandates like the Special rapporteur on the right to privacy, these developments together, including how requirements introduced for one purpose may create infrastructure or precedents usable for others.

These risks should also be assessed before services are launched, deployed in new jurisdictions, or connected to additional datasets, rather than relying exclusively on safeguards governing individual data requests or subsequent disclosures. Companies should assess their ability to resist demands that are inconsistent with international human rights standards, including where changes in national legislation or surveillance powers materially alter the risks to users. Such assessments should be revisited periodically and made subject to appropriate independent scrutiny. The risks associated with data access should also be assessed cumulatively. Information that may appear relatively innocuous in isolation can become significantly more sensitive when combined with identity credentials, location records, service histories, or other personal information held by public or private institutions. The Special Rapporteur should encourage states and companies to assess the implications of linking datasets and enabling secondary uses of personal information, rather than considering individual disclosures or data categories in isolation.

The UN Convention against Cybercrime is a significant development in this context. It establishes international cooperation mechanisms for investigating and prosecuting offences, including procedures for obtaining and sharing electronic evidence, which will operate alongside existing mutual legal assistance treaty (MLAT) processes and may reduce reliance on

the safeguards they provide. GNI has raised concerns about the Convention's broad scope, the limited and qualified nature of its human rights safeguards, and the risk that its provisions may be used against legitimate acts of expression by journalists, security researchers, vulnerable groups, and civil society, among others. Notwithstanding these risks and the Convention's slow rate of ratification, some member states are already pushing for a supplementary protocol to further expand the Convention's scope, instead of pursuing additional, necessary safeguards such as dual criminality, independent authorization, effective grounds for refusal, transparency, and effective remedies.

The Convention raises particularly acute concerns given the extent to which digital transnational repression is already accelerating. Governments are increasingly seeking to monitor, intimidate, or silence individuals beyond their borders through surveillance, requests for user data, and other legal and technical cooperation. Across regions, laws governing online content, intermediary liability, identity verification, and data access can interact with surveillance practices to expose journalists, human rights defenders, dissidents, and diaspora communities. Companies may also face conflicting legal obligations or pressure to comply with requests inconsistent with human rights standards. The Special Rapporteur should assess cross-border data-sharing frameworks for their effects on people at risk, and encourage states to ensure independent oversight, grounds for refusing law enforcement requests, user notification where possible, and effective redress.

Effective redress should extend beyond notification and the availability of grievance mechanisms. Depending on the circumstances, affected individuals should be able to obtain information about disclosures of their data, challenge inaccurate or misleading uses of that information, seek restrictions on further disclosure or processing, and obtain appropriate remedies for resulting harms. States and companies should also ensure that accountability is not extinguished by account deletion, changes in service ownership, or the withdrawal of a product, particularly where individuals may only discover the relevant disclosure or its consequences at a later stage.

Recent developments illustrate these dynamics. In Malaysia, the Communications and Multimedia Act grants broad powers to compel content removal and access communications under vague prohibitions, and the recently endorsed ASEAN Guidelines on the Governance of Digital Platforms risk facilitating coordinated regional enforcement based on expansive definitions of illegal content. Together, these measures risk lowering the threshold for cross-border identification and targeting of perceived government critics.

Government interventions in artificial intelligence

Governments are increasingly influencing the development and deployment of AI through legislation, regulatory guidance, public procurement, investment, and less formal forms of influence. These interventions can affect the entire AI value chain, from infrastructure and model development to the deployment of systems that shape access to information and public debate. GNI's Policy Brief on Government Interventions in AI provides a framework for examining these measures through a human rights lens, including their implications for privacy, freedom of expression, and non-discrimination.

Generative AI raises additional questions about the use of personal data to train and operate models, the processing and retention of user prompts and other data, and the potential impacts that stem from the sharing, exposure, or inferences of sensitive user information. At the same time, government measures to address harmful or misleading AI-generated content may affect people's ability to seek, receive, and impart information. Restrictions on AI outputs, mandatory monitoring, and obligations that encourage excessive filtering should be assessed against human rights standards rather than treated as necessary simply because they concern AI. GNI encourages the Special Rapporteur to examine, together with other Special Mandates like the Special rapporteur on the right to privacy, both the expression and privacy implications of AI-related data practices, as well as the effects of government interventions on expression, and to promote clear legal frameworks, transparency, accountability, and remedies.

These safeguards should be supported by clear implementation responsibilities and independent oversight, rather than relying solely on voluntary commitments or institutional assurances. Human rights assessments should identify the actors responsible for implementing safeguards, the resources and timelines required, and the mechanisms through which compliance can be independently verified. The Special Rapporteur should encourage states to ensure that appropriate safeguards are demonstrably operational before AI systems are deployed, and that there are effective mechanisms to suspend or remedy practices that give rise to human rights harms.

The human rights implications of AI deployment are particularly significant where individuals cannot meaningfully choose whether to interact with AI systems. Public authorities and other institutions may increasingly integrate AI into the provision of essential services, including healthcare, education, immigration, and social protection, leaving individuals with limited practical alternatives. The Special Rapporteur should encourage states and companies to ensure that accessible non-AI alternatives remain available where appropriate, that access to essential services is not unfairly restricted because an individual declines to use an AI-mediated channel, and that individuals can challenge consequential decisions without losing access to those services.

Age assurance and online safety

Age-assurance requirements illustrate the importance of assessing both the objectives of regulation and the means used to achieve them. Protecting children online is an important objective, and it is clear that more is needed from governments, platforms, and individuals in order to protect children's safety and rights. However, age-verification and age-estimation systems can require the collection or inference of sensitive personal information, reduce anonymity, introduce security risks, and restrict access to lawful information and services. These effects may extend to adults as well as children, and can be especially serious for people who rely on anonymity to seek sensitive information, communicate safely, or participate in public life.

These concerns are compounded by the spread of age-based access restrictions. Proposals to ban social media access for people under 16, as enacted in Australia, have prompted similar legislative initiatives in more than 60 other countries. Such bans are likely to drive greater reliance on age-verification technologies, and they risk unnecessarily restricting young people's access to online communities, information resources, and emergency services.

In our work on age assurance, including analysis of the rights implications of such requirements and feedback on Brazil's Preliminary Orientative Guide on Age Assurance Mechanisms, GNI has emphasized necessity, proportionality, data minimization, and safeguards against secondary use and excessive retention of assurance data. Design also matters: biometric methods should not become the default where less intrusive options exist, and users should not be excluded for lacking particular devices, connectivity, or identity documents. The Special Rapporteur should encourage states to assess the effects of age-assurance mandates on all users and to consider less intrusive, evidence-based approaches within broader child-safety measures. These concerns are also relevant to the risks facing human rights defenders identified in GNI's submission on protecting human rights defenders in the digital age.

2. Regional perspectives

- What are the three most pressing challenges to freedom of opinion and expression in your country, region, or area of work that you believe should receive greater attention from the mandate?

Drawing on our members' experience across regions, we highlight three challenges that we believe should receive greater attention from the mandate.

Broad content regulation and intermediary liability

GNI has documented a pattern of broad digital laws without sufficient safeguards against arbitrary or discriminatory enforcement, in response to legitimate concerns about cybercrime, security, online harms, or information integrity. Laws relying on imprecise terms such as "false information," "rumors," "defamation," or "public order" can leave authorities wide discretion and expose criticism, satire, investigative reporting, and other lawful expression to criminal or regulatory penalties. Even where prosecutions are less common, the threat of enforcement can chill expression, leading individuals, journalists, and platforms to self-censor.

Broad intermediary liability rules, short removal deadlines, and heavy penalties can encourage overcompliance and monitoring by tech companies. These risks are heightened when removal orders are issued outside of judicial processes, without clear reasons, or without notice to affected users, leaving little opportunity to seek review. GNI encourages the Special Rapporteur to promote clear and narrowly tailored definitions, proportionate penalties, realistic compliance timelines, transparency about government removal requests, and independent review of removal orders.

Recent examples illustrate these patterns. In India, GNI has raised concerns that draft amendments to the 2021 IT Rules, published in March 2026, would make compliance with a wide range of executive instruments, such as advisories and guidelines, a condition of safe harbour, collapsing the distinction between a lawful order and an administrative preference and encouraging over-removal. GNI has raised similar concerns about Sri Lanka's Online Safety Act, which establishes broad and vaguely defined categories of prohibited content, disproportionate penalties, and a commission with limited independence.

Surveillance, data access, and localization requirements

Similar risks arise where surveillance or electronic-evidence laws permit access to user data without independent authorization, limits on use, or opportunities to challenge demands, allowing data collected for one purpose to be reused for others. Data localization, licensing, and local-presence requirements can also increase government leverage over companies and place local staff at personal risk, while mandatory real-identity verification, as GNI has observed in Vietnam and Mexico, links online activity to individuals and weakens anonymity.

Network disruptions and website blocking

Network disruptions continue to be a significant issue, especially during elections but also around protests, examinations, and unrest. Whether full shutdowns, regional blackouts, or the blocking or throttling of specific services, they cut people off from information when access matters most, undermine participation, emergency services, and economic activity, and make it harder to document abuses. GNI has observed a significant increase in their use, including in Nepal in 2025, as well as recurring restrictions in Iran and Gaza. Additionally, more localized restrictions, such as on encrypted communications platforms in Russia are pushing people toward less secure or state-controlled alternatives.

Similar concerns arise from increasingly broad website-blocking orders. Governments, regulators, and, in some legal frameworks, private parties are increasingly ordering internet service providers to block specific websites on grounds ranging from alleged copyright infringement to national security and public order, with demands also extending to DNS resolvers, content delivery networks, and VPNs. These measures can have significant collateral effects: in Spain, IP-level blocking contributed to more than half a million domains becoming inaccessible over a five-month period, including media and nonprofit websites, as documented by OONI; and in France, a court order requiring Quad9 to block domains allegedly linked to piracy prompted the DNS resolver to withdraw its free service from the country, reducing access to an important privacy-enhancing tool that supports freedom of expression.

Disruptions are often justified on security, public order, or misinformation grounds, yet their legal basis is frequently unclear or unpublished, and operators and platforms may receive orders with little notice and limited ability to challenge them. GNI encourages the Special Rapporteur to reaffirm that disruptions are rarely, if ever, compatible with legality, necessity, and proportionality, to press for transparency about their legal basis and duration, and to call for accessible and effective redress, particularly around elections.

Please indicate your Region of work

☐ Africa

☐ Asia-Pacific States

☐ Eastern European States

☐ Latin American and Caribbean States (GRULAC)

☐ Western European and Other States (WEOG)

☐ Global

☐ Prefer not to say

☐ Other (please specify): _____

3. Maximizing Impact

- Looking ahead to the next three years, what actions, areas of engagement, or types of intervention would enable the mandate to have the greatest impact on the promotion and protection of freedom of opinion and expression?
- In your opinion, what emerging trends, technologies, governance developments, or changes are likely to have a significant impact on freedom of opinion and expression in the coming years from the perspective of the international human rights system?

Transparency and multistakeholder participation

GNI continues to emphasize advocacy for multistakeholder participation in tech governance at the national, regional, and global levels. Recent successes, including the World Summit on the Information Society (WSIS)+20's outcome and the Internet Governance Forum (IGF)'s permanent mandate, show that multistakeholderism remains a cornerstone of legitimate and effective digital governance. However, in other multilateral processes, including negotiations on the UN Convention against Cybercrime, the new Global Mechanism on developments in the field of ICTs in the context of international security and advancing responsible State behaviour in the use of ICTs, and the Global Dialogue on AI Governance, stakeholders continue to face barriers to access and participation. The Special Rapporteur is well placed to call on states to ensure that civil society, technical experts, academia, and the private sector can participate

meaningfully, including through accreditation, access to drafts and meetings, opportunities to comment, invitations to speak, visa and travel support, and other methods as set out in the NETmundial+10 Sao Paulo Principles. GNI's Multistakeholder Approaches to Participation in AI Governance (MAP-AI) project provides a relevant lens for these challenges, highlighting the importance of examining how multistakeholder participation can be meaningfully embedded in AI governance processes. These experiences underscore the need to move beyond formal commitments to inclusion and ensure that civil society, technical experts, and other affected stakeholders have practical opportunities to shape policy discussions and outcomes.

Limitations on multistakeholder participation are also often present in national law-making processes. GNI has commented on the lack of open and inclusive consultation in national digital policymaking, including in Bangladesh and Zambia. Civil society, already under strain, cannot easily engage in these processes, and a growing number of laws now target civil society organizations directly, including through registration and funding requirements that can restrict their ability to operate. GNI encourages the Special Rapporteur to promote consultation standards for digital legislation, including adequate notice, access to draft texts, impact assessments, and meaningful opportunities for public input, and to highlight laws that constrict the civic space needed to participate.

The mandate should also examine how responsibilities for protecting human rights are allocated across the wider digital service and deployment chain. In addition to governments and technology providers, this includes organizations procuring and deploying AI systems, public institutions integrating them into essential services, and other entities whose infrastructure or contractual arrangements influence how personal data is retained, accessed, or disclosed. Clear allocation of responsibilities is necessary to ensure that accountability is not weakened by fragmented institutional arrangements or the shifting of responsibility between different actors. The UN Guiding Principles on Business and Human Rights provide an important framework for examining these relationships and the corresponding responsibilities of each actor.

Meaningful participation and access to accountability mechanisms also require attention to language accessibility. Privacy notices, explanations of government data requests, disclosure notifications, and complaint and redress procedures should be accessible in the languages understood by affected communities. The availability of translated information alone may not be sufficient where individuals need to understand or challenge complex decisions affecting their rights. The Special Rapporteur should encourage states and companies to ensure that appropriate language assistance and, where necessary, competent human review are available throughout these processes.

Public Interest Digital Infrastructure

It is important to ensure media and civic actors participates in the policy discussions related to digital public infrastructure (DPI), and in particular the need to ensure that freedom of expression and media freedom, as referenced in the WSIS+10 Outcome Document and the Global Digital Compact (GDC), are addressed in ongoing and future policy development and in the building of DPI.

As developments at the UN level show, in particular the UN Universal DPI Safeguards Framework and UNDP's DPI safeguards work, along with similar initiatives across the ITU and national governments, DPI is a new opportunity to foster independent media and the free flow of information while preserving democratic resilience and integrity.

When built on open, interoperable and rights-respecting foundations, DPI can strengthen media independence by reducing reliance on a small number of private gatekeepers, opening new and more diverse revenue channels for media outlets, and improving journalists' access to public data, provided that strong safeguards prevent its use for surveillance, censorship or undue state influence over the press.

Looking ahead, GNI expects the greatest impact on freedom of opinion and expression to come from the convergence of the areas discussed above: cross-border cooperation frameworks, growing government interventions in AI, and safety-focused regulation that depends on collecting and verifying personal data. Each is often introduced for legitimate reasons, but together they may build infrastructure for surveillance and control that outlasts its original purpose. We encourage the mandate to monitor these developments across processes and regions and to provide states with practical guidance grounded in human rights standards.

GNI thanks the Special Rapporteur for the opportunity to contribute and remains keen to engage with the mandate throughout its term. We would welcome opportunities to share further information from our members and our policy work, to participate in consultations and country visits where helpful, and to support the Special Rapporteur's efforts to advance freedom of opinion and expression in the digital age.