

GNI Submission to the Global Digital Compact Consultation

The Global Network Initiative (GNI) welcomes the opportunity to submit input to the intergovernmental process on the Global Digital Compact. GNI has held multiple discussions with our full membership to inform the development of this submission, and we are pleased to be able to share core principles and commitments we hope to see reflected in the Global Digital Compact.

GNI's perspective is informed by over a decade and a half of experience undertaking multistakeholder collaboration to advance the [GNI Principles on Freedom of Expression and Privacy](#) and corresponding [Implementation Guidelines](#) (together, the GNI framework). The framework provides guidance on how information and communication technology (ICT) companies can build appropriate policies, systems, and capacity to advance responsible decision-making in response to government pressures, restrictions, or demands. GNI's expert members work together to uphold and promote this framework around the world, assess implementation of the framework by companies through our unique assessment process, participate in shared learning on related issues, challenges, and opportunities, and engage in policy advocacy in support of rights-respecting laws and policies.

GNI members include 90 leading digital rights and press freedom groups, information and communications and technology companies, investors, and academics. This experience guiding company action, undertaking shared learning, and engaging on laws and regulations across four policy areas — network disruptions, privacy and surveillance, jurisdictional assertions and limits, and content regulation — has offered valuable insights that can help guide all stakeholders in developing shared frameworks to help preserve a free, open, and secure Internet.

The GNI framework is centered on the rights to freedom of expression and privacy, and is consistent with the foundations of the broader UN Guiding Principles on Business and Human

Rights (UNGPs) and international human rights law. Our submission focuses on GNI’s core commitments to freedom of expression and privacy, while emphasizing areas where the framework can provide guidance on policies and practices for addressing the full range of human rights, as well as issues where our policy and learning experiences offer insights for broader digital governance and policymaking with a human rights lens. Accordingly, we have organized the submission around core principles to preserve digital rights, and then spelled out specific commitments for companies, governments, and all stakeholders.

At the core of GNI’s mission, governance, and work is a commitment to the inclusion of a broad diversity of voices and views and a shared belief in the values and principles established in international human rights law. We strongly encourage the co-chairs of the intergovernmental process, Member States, and all actors contributing to the multistakeholder technology track to ensure that the process and substance of developing the Global Digital Compact reflects this approach.

1) Focus Area: Applying Human Rights Online

Principles

- The [GNI Principles on Freedom of Expression and Privacy](#) and corresponding [Implementation Guidelines](#) provide a framework for responsible company decision making and multistakeholder engagement to advance freedom of expression and privacy in the ICT sector. This framework covers:
 - governance and oversight of freedom of expression and privacy risks and opportunities, i.e., “integrating the Principles into company DNA”;
 - ongoing human rights due diligence (HRDD) and risk management, in line with guidance detailed in the UNGPs;
 - policies and practices to assess and respond to government restrictions, demands, and requirements that impact freedom of expression and privacy;

- transparency and engagement to inform stakeholders about companies' policies and practices and promote the framework
- The GNI Principles are rooted in the [United Nation Guiding Principles on Business and Human Rights](#) (UNGPs) and International Human Rights Law, which should remain core to any new principles and frameworks developed for an open, free, and secure digital future for all.
- The rights to freedom of expression and privacy should not be restricted by governments, except in narrowly defined circumstances based on internationally recognized laws or standards.
 - Where governments seek to implement laws and regulations that might contribute to such restrictions, human rights principles can help them find creative and appropriate ways to engage stakeholders, design fit-for-purpose regulations, and mitigate unintended consequences.
- The state duty to protect human rights under the UNGPs builds on the obligation not to infringe upon human rights directly and includes both a duty to protect against human rights abuses by third parties, and a duty to ensure legal frameworks do not constrain but enable business respect for human rights.
- The principle of non-discrimination should be reflected in any content governance or regulation efforts.
- Multistakeholder engagement is a foundational principle in the history of global Internet governance that should be at the core of any additional efforts to set international norms and standards.
- There is a need for improved, meaningful digital transparency from digital communications companies as well as from governments and regulators in this space.

Commitments

For Companies

- Companies should commit to upholding human rights, including by implementing the UNGPs and the GNI Principles. GNI member companies commit to periodic independent assessment of their efforts to implement these principles with improvement over time via GNI's unique [accountability mechanism](#).
- The GNI framework is focused on freedom of expression and privacy, but provides relevant guidance for addressing the full range of human rights risks and opportunities, including through the establishment of corporate commitments to human rights, developing comprehensive HRDD processes, engaging relevant stakeholders, practicing meaningful transparency, and providing appropriate senior/board-level oversight of these commitments and activities.

For Governments:

- Governments considering proposals to address concerns about digital content and conduct should incorporate the guidance detailed in the GNI *Content Regulation & Human Rights Policy Brief* ([CRPB](#)). Governments should conduct careful, public, and participatory deliberation on such proposals, and include strong transparency and accountability measures for relevant oversight or enforcement bodies.
- The CRPB details steps governments can take to uphold the human rights principles of legality, legitimacy, and necessity and proportionality, including:
 - Legality – States should refrain from: using vague and reductive definitions that would incentivize over-removal; prohibiting categories of expressive conduct or content without engaging in a transparent and participatory process of debate; outsourcing adjudication of expression to private companies without providing appropriate clarity on interpretation and application of the law; or shifting legal liability from authors to intermediaries for illegal content generated by users.
 - Legitimacy – States should refrain from allowing laws and/or regulation to result in discriminate against content based on medium.
 - Necessity – States should refrain from: applying legal requirements on platforms without considering their relative size, capabilities, and business models;

imposing strict timelines for removal of content without regard to context, potential unintended consequences, and the value of prioritization; imposing preemptive filtering or general monitoring requirements; or making intermediaries liable for specific content moderation decisions.

For All Stakeholders

- Where the Global Digital Compact may speak to potential regulatory approaches, we encourage the promotion of first principles, key safeguards, and flexible guidance, as opposed to more rigid regulatory frameworks that can be misconstrued to justify undue restrictions and will have different implications and impacts in distinct jurisdictions depending on context, including resourcing and rule-of-law adherence.
- The Global Digital Compact consultations and ultimate output should explore avenues to reinforce and build upon existing efforts to empower multistakeholder processes and support work toward a free, open, interoperable, and secure Internet, such efforts being undertaken through the Internet Governance Forum (IGF), the [Christchurch Call](#), the [Freedom Online Coalition](#), and the [Action Coalition on Meaningful Transparency](#).
- Continue to build on efforts to identify good practices for meaningful and inclusive stakeholder engagement on digital rights issues.

2) Focus Area: Avoiding Internet Fragmentation

Principles

- With increasing regulatory scrutiny of ICTs around the world, international human rights law offers time-tested guidance that can help align these efforts and provide clarity and predictability for governments, companies, and individuals around the world.
- The GNI Principles and Implementation Guidelines make clear that ICT companies should comply with all applicable laws and respect internationally recognized human rights, wherever they operate.

- If national laws, regulations, and policies do not conform to international standards, the GNI framework details steps to avoid, minimize, or otherwise address the adverse impact of government demands, laws, or regulations, including:
 - Requiring governments to follow established domestic laws and legal processes;
 - Interpreting government requests narrowly, including regarding the requesting government's jurisdiction;
 - Proactively engaging with governments to encourage laws, regulations, requirements, restrictions, and demands that are consistent with international laws and standards;
 - Seeking the assistance, as needed, of relevant government authorities, international human rights bodies, or non-governmental organizations.
- Government-ordered network disruptions are drastic measures that almost always violate the principles of necessity and proportionality, often occurring during moments of political sensitivity or importance. Disruptions pose significant risks for human rights, as well as economic and social wellbeing.
- A small but growing number of governments also seek to implement [measures](#) centralizing state control over internet infrastructure, an approach that warrants opprobrium.
- Companies that hold user data can and should play an important role in scrutinizing and resisting improper, unnecessary, or disproportionate government demands. GNI recognizes that clear, rights-respecting, and efficient mechanisms for cross-border data sharing for the purposes of criminal investigations can help mitigate the risk of more restrictive alternatives, such as circumventing normal legal process to access user data or compelling data localization.
 - GNI encourages bilateral, multilateral, and multistakeholder approaches that facilitate responses by companies who hold data abroad, where appropriate, to governments whose laws and procedures meet relevant international human rights standards.

- Data localization measures can pose privacy risks when paired with disproportionate authorities for governments to access user data stored in a country. By creating single points of failure and targets for attacks, they can also increase cybersecurity risks.
- Opaque, arbitrary government surveillance practices can contribute further to Internet fragmentation, creating mistrust and limiting access to cross-border mechanisms.

Commitments

For Companies

- In line with the guidance from the GNI framework, companies should continue to take steps to avoid, mitigate, or otherwise address potential adverse human rights impacts from laws, policies, and government demands that are likely to reinforce Internet fragmentation.
- This includes multistakeholder advocacy to encourage governments and international institutions to adopt policies and practices that are consistent with and advance the GNI Principles.

For Governments

- Governments must refrain from the use of state-sponsored internet shutdowns and disruptions, and support multilateral engagement, including via the Freedom Online Coalition, to curb their use and mitigate their impacts.
- Governments should commit to preserving the free flow of data across borders where appropriate safeguards exist to address potential cybersecurity or human rights risks.
- When seeking to address concerns about digital content and conduct, in line with the guidance in the CRPB, governments should target interventions to services and situations that generate significant risk of harm. This means carefully considering the types of services, at which layers in the ecosystem, that are appropriately positioned to address the specific concerns at issue, recognizing the consequences of such interventions may differ significantly from one type of service to another.

- In looking to establish new mechanisms or update existing mechanisms for sharing digital evidence across borders for criminal investigations, governments should ensure the following principles are included to protect human rights: prior authorization of requests; focus on serious crimes; availability of meaningful redress; transparency regarding the number, type, and scope of the requests; and oversight and accountability.
- GNI recently expressed [concerns](#) about efforts from governments to ban or otherwise eliminate access to specific digital communications platforms. While governments may have legitimate concerns about the impact of digital content and conduct on specific platforms, completely blocking entire platforms, services, or mediums is almost never a necessary or proportionate response to such concerns.
- Regulators should continue to identify spaces to strengthen shared values and alignment on rights-respecting regulations.

For All Stakeholders

- Build capacity for and increased engagement with digital rights experts in global Internet governance conversations, including in standards bodies.

3) Focus Area: Promoting Artificial Intelligence

Principles

- As detailed in the GNI framework, consistent with the UNGPs, and considering international human rights standards, participating companies will carry out HRDD to identify, prevent, evaluate, mitigate and account for risks to the freedom of expression and privacy rights that are implicated by the company's products, services, activities and operations.
 - Where HRDD identifies circumstances where freedom of expression and privacy may be jeopardized or advanced, GNI companies commit to employ human rights impact assessments (HRIAs) and develop effective risk mitigation strategies as appropriate.

- Designing and introducing new technologies, products, and services, and their use, is one area where HRDD has previously revealed the need for HRIAs.
- Among other good practices, HRIAs should be prioritized where risks of adverse impacts are most salient, should be updated over time, and should draw upon insights from a variety of sources.
- GNI companies also commit to use best efforts ensure that business partners, investments, suppliers, distributors, and other relevant related parties follow these Principles.
- Recognizing the constant change in the ICT sector, GNI's multistakeholder membership commit to undertaking shared learning on contemporary freedom of expression and privacy challenges, including considerations around new and emerging technologies and the GNI framework.
- All stakeholders should give particular care to the potential freedom of expression risks associated with automated tools for content moderation;
 - Requirements for companies to proactively filter types of harmful content require significant human rights scrutiny.
- We support the risk-based approach taken by various national and multilateral initiatives considering legal frameworks for AI, which target the uses of artificial intelligence that offer the most salient risks and tailor requirements for identifying, preventing, and mitigating risks accordingly.
- The application of artificial intelligence by public actors, including law enforcement, deserves at least as much, if not more, scrutiny as commercial applications in any regulatory framework. Requirements for privacy risk assessments or HRDD or HRIA should apply equally to commercial and public uses.

Commitments

For Governments

- Whether governments are deploying AI-enabled technology directly, or requiring or incentivizing its use by other actors, it is critical that they continue to ensure that the development, design, and deployment of such technology is conducted transparently, informed by stakeholder input, and governed by adequate transparency and accountability. Without sufficient and appropriate governance frameworks that allow for independent scrutiny, risk identification and mitigation, public awareness and education, individual choice/ability to opt-out, and appropriate remedy, public trust will be undermined and the potential benefits of AI-enabled technologies will be jeopardized.
- Governments must take a more active role in developing safeguards, such as robust transparency, accountability, and oversight mechanisms, regarding the use of AI-enabled technologies for law enforcement and surveillance purposes. This includes particular attention to the privacy and data protection risks associated with the collection of biometric data.
- Governments seeking to regulate AI should ground such efforts in international human rights law, which provide an important baseline from which to analyze risks and opportunities effectively, to define key safeguards and proportionate approaches, and to help ensure that myriad efforts at national, regional, and international levels to regulate AI are in sync.

For Companies

- Companies must ensure that their development and use of AI-enabled technology, including the sale of such technologies, is consistent with their responsibility to respect human rights, including the right to privacy. GNI's multistakeholder framework offers a model for the ICT sector to ensure respect for privacy and freedom of expression in their products, services, and operations, including those utilizing AI.
- As detailed in the data protection section below, companies must employ protections with respect to personal information in all countries where they operate.

For All stakeholders

- Inclusive and diverse multistakeholder engagement should be core to any normative efforts and their promotion. All stakeholders must pay particular attention to the impacts on marginalized groups when considering regulating or implementing AI technologies.
- GNI strives to continue fostering shared learning and expert engagement on AI issues, including potential discussions on generative AI.

4) **Focus Area: Protect Data**

Principles

- The GNI Principles on Freedom of Expression and Privacy and corresponding Implementation Guidelines call on companies to employ protections with respect to personal information in all countries where they operate in order to protect the privacy rights of users in the face of government demands and restrictions.
- The GNI framework encourages participating companies to disclose, to the extent allowed under the law, what laws and policies compel them to provide personal information to government authorities, what personal information the participating companies collect, and the company's policies and procedures for responding to government demands (see more about these policies and practices in the "Internet Fragmentation" section).
 - The framework also details that participating companies will assess the human rights risks associated with the collection, storage, and retention of personal information in the jurisdictions where they operate and develop appropriate mitigation strategies to address these risks.
- GNI encourages companies to adopt policies and procedures that address situations where governments may make demands through proxies and other third parties to evade domestic legal procedures.

- Government surveillance activities must comply with principles of rule of law and democratic governance, as well as human rights principles such as legality, necessity, and proportionality.
 - GNI has [documented concerns](#) about legal and technical arrangements that allow government authorities to access data streams directly – that is, without having to request access from, or even notify, the service providers that collect and/or transmit the data as part of their services. By taking operators “out of the loop,” these “direct access” arrangements remove a critical potential safeguard for user privacy.
- Governments and regulators considering new or updated data protection laws must also center human rights in their design. This includes not only ensuring strong foundations for privacy and data protection, but avoiding some of the risks and pitfalls GNI has seen in recent approaches, which include: overly broad exceptions for public actors and/or national security purposes; using data protection to expand surveillance authorities; insufficient independence and oversight of new regulatory bodies; or unnecessary limits on cross-border data flows (see “Internet Fragmentation” section above).

Commitments

For Companies:

- Companies should assess the human rights risks of data collection and storage practices in jurisdictions on an ongoing basis and develop mitigation strategies, as described in the GNI framework.
- Companies should seek to be transparent about the laws and regulations that may authorize access to user data, including via resources like the GNI [Country Legal Frameworks Resource](#), and to share statistics about the demands they face to the extent the law allows.

For Governments

- Lead by example by committing to data protection approaches that consider responsibility for public actors and/or avoid broad exemptions for those actors.
- Collection and processing of data by governments should be subject to clear and meaningful safeguards:
 - Any exemptions must be narrowly defined, subject to the principles of necessity, proportionality, and legality consistent with international human rights standards.
 - Governments should commit to strict standards for access to user data, such as independent judicial authorization, avenues for oversight and transparency, and remedial measures.
 - Governments should provide notice to surveillance targets when notification won't unduly impact investigations, and avoid undue restrictions on companies providing notice.
 - Governments should not only enable company transparency around government demands, but law enforcement and executive bodies should also model transparency measures to complement these company efforts.
- Governments should address potential legal loopholes that can enable government procurement of user data via third parties.
- Governments should avoid introducing legal frameworks enabling direct access. Where these authorities exist already, they should at minimum: (i) provide sufficient authorization procedures, supervision, and remedy so as to ensure that surveillance conducted is proportional to the purpose for which it is authorized and provide effective guarantees against abuse; (ii) allow companies to disclose information about interception and access to data on their networks; and (iii) ensure that such access is disclosed to the subject in a timely manner if that data is used in any civil, administrative, or criminal proceeding.

- Governments should also strengthen export controls for technologies that are intended for use in direct access in countries with repressive track records, in line with UNGPs.

For All Stakeholders

- As laws and regulations envision new mechanisms for data access for researchers, an admirable transparency aim, there is an important responsibility to put forth good guidance on related data protection measures as well.
- All stakeholders should advocate for expanded transparency, oversight, and accountability of laws, regulations, and actions related to communications surveillance.