



## **GNI Submission to the High Commissioner Report on the Practical Application of the UNGPs in the Technology Sector**

### **1. Introduction**

The Global Network Initiative (GNI) welcomes the opportunity to engage with the Office of the High Commissioner for Human Rights (OHCHR) on the practical application of the UN Guiding Principles on Business and Human Rights (UNGPs) to the activities of technology companies ahead of the March 7–8 [consultation](#) and subsequent thematic report to the Human Rights Council.

[GNI](#) brings together over 80 prominent academics, civil society, information and communications technology (ICT) companies, and investors from around the world. Members' collaboration is rooted in a shared commitment to the advancement of the [GNI Principles on Freedom of Expression and Privacy](#), which are grounded in international human rights law and the UNGPs. For over a decade, the GNI Principles and corresponding [Implementation Guidelines](#) have helped ICT companies avoid and mitigate risks to freedom of expression and privacy in the face of government laws, restrictions, and demands. GNI and its membership are grateful to have participated in regular multistakeholder [engagement](#) led by the OHCHR B-Tech project in each of the focus areas of the consultation. In this submission we will share applicable elements of the GNI framework and lessons learned from GNI's multistakeholder collaboration, including through shared learning, collective [policy engagement](#), and GNI's independent [company assessments](#).

## 2. Human Rights Due Diligence and End-use

The GNI Principles and corresponding Implementation Guidelines detail a broad set of commitments that enable ICT companies “to avoid or minimize the impacts of government restrictions on freedom of expression and information,”<sup>1</sup> and to “employ protections with respect to personal information in all countries where they operate in order to protect the privacy rights of their users.”<sup>2</sup> This includes carrying out ongoing human rights due diligence to identify, prevent, evaluate, mitigate and account for risks to the freedom of expression and privacy rights that are implicated by a company’s products, services, activities and operations.<sup>3</sup> The Principles and Implementation Guidelines provide further recommendations for companies’ structures and processes to ensure ongoing HRDD and GNI commitments more broadly are effectively integrated in company analysis, decision making, and operations.<sup>4</sup>

Where HRDD identifies circumstances where freedom of expression may be jeopardized or advanced, the GNI Principles and Implementation Guidelines also call on participating companies to employ human rights impact assessments (HRIAs) and develop effective risk mitigation strategies as appropriate. Companies should undertake HRIAs early enough to “inform the development of a new activity or relationship,” and HRIAs and other due diligence processes should be ongoing, with companies “tak[ing] appropriate action to avoid, mitigate or in other ways address potential negative human rights impacts on an ongoing basis,” and “updating HRIAs over time, such as when there are material changes to laws, regulations, markets, products, technologies, or services.”<sup>5</sup>

---

<sup>1</sup> GNI Principles, “Freedom of Expression,” available at <https://globalnetworkinitiative.org/gni-principles/>

<sup>2</sup> GNI Principles, “Privacy”

<sup>3</sup> GNI Implementation Guidelines, e.g., guidelines 2.4–2.7. Available at <https://globalnetworkinitiative.org/implementation-guidelines/>

<sup>4</sup> GNI Principles, “Responsible Company Decision Making,” Implementation Guidelines, e.g., guidelines 2.1–2.4, 2.12–2.13.

<sup>5</sup> GNI Implementation Guidelines, guideline 2.7

The Implementation Guidelines detail scenarios where this ongoing HRDD has revealed the need for HRIAs, while recognizing that HRIAs are “undertaken to different levels of detail and scope depending on the purpose of the impact assessment.” Such scenarios include, but are not limited to, market exit/entry; corporate due diligence on potential partners, investments, suppliers, and other relevant related parties; designing and introducing new technologies, products, and services and their use; and acquiring other companies or forming operational partnerships.<sup>6</sup>

The Implementation Guidelines recognize the influence of participating companies will vary across different relationships and contractual arrangements. Companies commit to implementing these Principles wherever they have “operational control.” When they do not, participating companies will use best efforts<sup>7</sup> to ensure that business partners, investments, suppliers, distributors, and other relevant related parties follow these Principles, and prioritize circumstances related to third party relationships where the risks to freedom of expression and privacy are most salient.<sup>8</sup>

GNI’s assessment process, shared learning, and stakeholder engagement have demonstrated some of the challenges and complexities presented by HRDD and HRIAs in the ICT sector. First, there is a need for a more holistic view of the sector-wide impacts and interrelationships between different layers of the “ICT stack.” As Dunstan Allison-Hope at Business for Social Responsibility (BSR) has [written](#), “While today’s human rights assessments are typically undertaken for a single company, in the technology industry, the solutions often need to be

---

<sup>6</sup> GNI Implementation Guidelines, guideline 2.6

<sup>7</sup> The GNI Principles define “best efforts” as: “The participating company will, in good faith, undertake reasonable steps to achieve the best result in the circumstances and carry the process to its logical conclusion.”

<sup>8</sup> GNI Principles, “Multi-stakeholder collaboration.” GNI Implementation Guidelines, e.g., guidelines 2.6–2.11

applied at the system level.” In addition, the [public report](#) on the 2018/19 cycle of GNI independent company assessments identified “HRDD on research and development and product design, as well as collective work by GNI members to inform HRDD on emerging technological challenges,” as areas for further learning.<sup>9</sup> Finally, while there has been much discussion in the business and human rights community on the relationship between HRDD and HRIAs, GNI’s most recent assessment process demonstrated the value of both fully fleshed HRIAs, undertaken for various purposes, and processes fit for more rapid, targeted deployment.<sup>10</sup>

GNI is undertaking various efforts to foster learning and develop additional tools specific to the ICT sector. GNI recently established a dedicated HRDD working group, deliberating with members on areas where modular tools and guidance for HRDD and HRIAs are needed. Further to these discussions, GNI recently entered into an agreement with Business for Social Responsibility (BSR) to develop a framework for mapping the ICT ecosystem to improve the ability of companies and other actors to identify, understand and appropriately address human rights risks, including how the relationships between different actors can affect leverage, exposure, and collaboration. GNI and BSR are also sharing insights and outputs with other, non-GNI stakeholders through participation in the [Action Coalition for Responsible Technology](#) (ART) under the auspices of the Danish [Tech for Democracy](#) initiative.<sup>11</sup> GNI has also explored particular [considerations](#) where States act as purchasers, end users, or beneficiaries of digital technologies.

---

<sup>9</sup> Public Report on the Third Cycle of Independent Assessments of GNI Company Members 2018/19, page 103. Available at <https://globalnetworkinitiative.org/wp-content/uploads/2020/04/2018-2019-PAR.pdf>

<sup>10</sup> *Ibid*

<sup>11</sup> GNI and BSR join the Danish Institute for Human Rights, the UN Human Rights B-Tech Project, Ericsson, and Telia Company on the steering group for the ART. In addition to ecosystem mapping, the other current ART workstreams revolve around identifying good practices for stakeholder engagement on digital technologies (led by B-Tech), and assessing policy coherence among different human rights-related regulatory developments of digital technologies (led by DIHR)

### 3. The State Duty to Protect, or Regulatory and Policy Responses

Consistent with the UNGPs, the GNI Principles recognize that companies “should comply with all applicable laws and respect internationally recognized human rights, wherever they operate.”<sup>12</sup> However, as GNI’s most recent assessment cycle demonstrated, “[w]hether it is governments who are genuinely committed to human rights but facing vexing challenges around disinformation, cybercrime, hate crimes, or terrorism, or governments who are actively seeking to suppress their citizens’ rights, the operating environment for rights-respecting ICT companies is getting more complex.”<sup>13</sup> The [2021 Freedom on the Net Survey](#) found a “growing number of governments are asserting their authority over tech firms, often forcing the businesses to comply with online censorship and surveillance.”

We appreciate that States should take steps to address legitimate concerns related to national security, anti-discrimination, privacy, and the rights of children. Unfortunately, we have [documented](#) a number of regulatory efforts, nominally intended to address these concerns, that instead add difficulty for intermediaries in respecting the rights of their users. Some of the more alarming trends include broad and vague definitions and scope; overly excessive penalties, including significant liability for company personnel; and requirements to remove content under strict timelines or via automated tools without attention to necessary safeguards. Furthermore, some proposals could lead to arbitrary or unlawful infringements on user privacy, including through so-called “tracing” requirements that threaten anonymity and encryption. While there are no off-the-shelf solutions to concerns about digital content and conduct, in GNI’s [Content Regulation and Human Rights Policy Brief](#), we outline a set of [recommendations](#) rooted in upholding the principles of legality, legitimacy, and necessity in

---

<sup>12</sup> GNI Principles, e.g., “Preamble”

<sup>13</sup> Public Report on the Third Cycle of Independent Assessments of GNI Company Members 2018/19, page 103



order to ensure protection of freedom of expression and privacy, informed by review of two dozen approaches and multistakeholder expert consultations in multiple regions.

With these growing legal and regulatory pressures, the GNI framework provides guidance for companies in how to “honor the principles of internationally recognized human rights to the greatest extent possible,” and to “avoid, minimize, or otherwise address the[ir] adverse impact” and “be able to demonstrate their efforts in this regard.”<sup>14</sup> As increasingly assertive demands and restrictions might emerge, the framework details steps for responsible company decision making to mitigate and avoid human rights risks, such as encouraging specific demands, seeking assistance from relevant bodies and challenging overbroad demands as appropriate, and communicating with users when required to implement restrictions or share data, wherever possible.<sup>15</sup> When implementing the Principles, companies will always seek to ensure the safety and liberty of company personnel who may be placed at risk.<sup>16</sup> In addition, GNI members undertake collaborative engagement in support of laws and policies that promote and protect freedom of expression and privacy, and enable companies to respect these rights.<sup>17</sup>

GNI has long advocated for expanded transparency, oversight, and accountability with respect to laws, regulations, and policies related to [communications surveillance](#), in order to protect privacy and ensure respect for the rule of law and democratic governance. GNI members commit to being as transparent as possible about the requests they receive from law enforcement and intelligence agencies for access to user data, as well as related laws and regulations that might authorize access. One mechanism for enhancing transparency is through contributions to the [GNI Country Legal Frameworks Resource](#), which maps pertinent legal

---

<sup>14</sup> GNI Principles, e.g., “Preamble”

<sup>15</sup> GNI Principles, e.g. “Freedom of Expression,” “Privacy,” “Responsible Company Decision Making,” GNI Implementation Guidelines, eg., guidelines 3.1–3.3, 3.5

<sup>16</sup> GNI Principles, “Responsible Company Decision making,” GNI Implementation Guidelines, guideline 2.3

<sup>17</sup> GNI Principles, e.g., “Multi-stakeholder Collaboration,” GNI Implementation Guidelines, e.g., guidelines 4.1–4.9



powers that could authorize government censorship or surveillance activities in over 55 countries. In June 2021, GNI issued a statement on “[direct access](#),” calling for more transparency and dialogue around legal and technical arrangements that allow government authorities to access data directly – that is, without having to request access from, or even notify, the service providers that collect and/or transmit the data.

As [DIHR](#) and others have shown, there is a notable uptick in regulations that seek to introduce specific legal requirements for due diligence and assessment of ICT companies’ human rights and other societal impacts. These approaches can help ensure that companies develop, carry out, and are transparent about their internal policies for risk assessment and mitigation. However, as regulations reference concepts like due diligence, risk assessment, and impact assessment, and envision audits or other regulatory mechanisms for verification, it is imperative that regulators strive to align their approaches with the significant body of existing guidance and practice that have been developed alongside the UNGPs.

In September 2021, GNI and the Center for Democracy and Technology partnered to hold a workshop and public event focusing specifically on [HRDD and the Digital Services Act](#). These discussions examined the risk assessment provisions of the DSA, and featured representatives from EU bodies and Member States, as well as academia, civil society, and the private sector. Roundtable participants reflected on the need to ensure that any liability regimes paired with due diligence obligations are proportionate to the risks faced by covered services; maintain sufficient flexibility, as emphasized in the UNGPs, to account for different business models and risk profiles; and avoid “ticking the box” exercises, where regulations add additional reporting or assessment requirements that have little bearing on companies’ human rights impacts in practice.



#### **4. Accountability and Remedy**

The GNI [independent company assessment](#) offers a unique process for reviewing ICT companies' efforts to implement their freedom of expression and privacy commitments. Learning and trust established through this process helps foster collaboration among members to improve company practices. Confidential by design, the assessment methodology allows GNI's civil society, academic, and investor board members insight into these practices, allowing for discussion of sensitive cases and internal company systems and processes. Based on a detailed evaluation of confidential reports prepared by independent assessors, and interviews with assessors and member companies, the GNI Board is tasked with determining whether each member company has “made good-faith efforts to implement the GNI Principles with improvement over time” during the period covered by the assessment.

The assessment process allows non-company members to raise concerns about particular company decisions and scenarios, identifying individual case studies that must either be incorporated into the report or otherwise addressed by the company concerned. The results of each cycle of assessments are shared publicly in GNI's public assessment report, with individual companies required to communicate the assessment results separately. GNI is currently undergoing its fourth cycle of independent assessments, and further information on this and past cycles is available [here](#).

In addition to the assessment process, the GNI Implementation Guidelines call on member companies to “establish[] grievance mechanisms for users to make it possible for grievances about issues related to freedom of expression and privacy to be communicated to the company for consideration,” and where a company determines its business practices are inconsistent



with the Principles or have caused or contributed to adverse impacts, remediation.<sup>18</sup> Outside of the assessment process, GNI’s shared learning function allows members to raise concerns about sensitive topics directly with staff and members and to facilitate candid conversations guided by the GNI framework.

## **5. Human Rights Risks in Business Models**

As we have detailed throughout this submission, the GNI framework offers a roadmap, grounded in the UNGPs and international human rights law, for embedding a commitment to respect the rights to freedom of expression and privacy and privacy into ICT companies’ DNA. This includes, among other steps, ensuring oversight of implementation of the principles at the highest levels of the company<sup>19</sup>, documenting corresponding policies and implementation, and integrating the Principles into company culture and training processes. The GNI framework helps companies understand and address the potential impacts of their business models, value chains, and product development, and offers a trusted platform to reflect on these considerations with GNI’s non-company experts. The diversity of companies that participate in GNI, ranging from equipment vendors to web infrastructure providers, to telecommunications service providers, to search engines and social media platforms, heightens members’ collective understanding.

While the GNI framework offers a helpful roadmap, as the use of digital platforms and services expands across the globe, so too does the need to better understand how they operate and how companies and governments collect and use the data that they generate. Despite broad agreement on the need for more and better transparency, related conversations often miss important perspectives and there is a surprising lack of consensus on what exactly transparency

---

<sup>18</sup> GNI Implementation Guidelines, guideline 2.13. The application guidance further details that companies should align the design of their mechanisms with the effectiveness criteria set out in Principle 31 of the UNGPs

<sup>19</sup> GNI Principles, “Responsible Company Decision-Making,” Implementation Guidelines, e.g., guidelines 2.12-2.13



means in the digital context. In order to help identify opportunities, foster collaboration, and enhance the role of groups from underrepresented regions in transparency-related efforts, GNI has convened a group of globally diverse organizations<sup>20</sup> to develop a new [Action Coalition on Meaningful Transparency \(ACT\)](#), under the Danish Tech for Democracy initiative. In the coming months, the ACT aims to bring together a wide range of academics, civil society organizations, companies, governments, and international organizations to work collaboratively on digital transparency.

## 6. Conclusion

The GNI framework offers practical guidance for ICT companies on implementing their commitments to respecting the rights to freedom of expression and privacy and for multistakeholder collaboration to respect and advance these rights. As we have detailed in this submission, global legal and regulatory developments have added to pressures ICT companies face to restrict access to content and services and share user data, even as many policymakers seek to address legitimate regulatory concerns. The work of the OHCHR in documenting the application of the UNGPs to technology companies is a valuable step toward developing a shared understanding to inform laws and policies that enable, as opposed to constrain, ICT companies' abilities to respect their users' rights. We appreciate the opportunity to share GNI's related multistakeholder experiences and insights and we look forward to future engagement on these critical topics.

---

<sup>20</sup> Current ACT Steering Group members include: the Center for Democracy & Technology, the Center for Technology & Society at Fundação Getulio Vargas, the Centre for Communications Governance at the National Law University Delhi, the Centre for International Governance Innovation, the Digital Forensic Research Lab, the Global Network Initiative, the Institute for Strategic Dialogue, and the Partnership for Countering Influence Operations at the Carnegie Endowment for International Peace. Suggested outputs from the ACT include (i) clarifying relevant definitions and terminology; (ii) mapping existing and identify missing efforts; (iii) sharing lessons learned; (iv) identifying opportunities for alignment and coordination; and (v) producing recommendations for companies, donors, researchers, and governments.