GNI Submission to the Special Rapporteur Report on Freedom of Expression in Times of Armed Conflict and other Disturbances

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 challenges to freedom of opinion and expression in times of armed conflict and other disturbances to inform the Special Rapporteur's scoping report for submission to the 77th session of the UN General Assembly in October 2022.

GNI brings together over 80 prominent academics, civil society organizations, 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 UN Guiding Principles on Business and Human Rights (UNGPs). For over a decade, the GNI Principles and corresponding Implementation Guidelines have guided ICT companies to assess and mitigate risks to freedom of expression and privacy in the face of laws, restrictions, and demands, including in countries experiencing or recovering from conflict and other politically-sensitive contexts where violence may occur.

2. GNI's Working Methods

GNI fosters a range of opportunities for its diverse membership to come together and discuss matters related to freedom of expression and privacy in the ICT sector. These include opportunities to discuss company-specific case studies in the context of our confidential, independent

assessment, timely "shared learning" calls, which may include non-GNI member experts, and discussions designed to produce policy statements and other outputs that articulate positions representing the consensus views of our members.

In recent years, GNI has had many opportunities to examine the GNI Principles and the UNGPs in various active and post-conflict settings. As a wider range of expression, including political expression, has increasingly migrated online, ICT companies present or otherwise providing services in countries experiencing violent conflict face an increasingly challenging set of situations, questions, and demands. These sensitive scenarios often lead to pressures, including legal demands, on companies that can make it difficult for them to adhere to relevant human rights principles. During conflicts and politically sensitive moments, state actors are often more likely to encourage, facilitate, and implement requirements for censorship or access to user data, sometimes accompanied by threats to the safety of local personnel. In these contexts, states are also more likely to attempt to misuse ICT products and services, including in order to manipulate relevant information spaces, or surveil certain groups, including human rights defenders, among other measures.

In this submission we will share applicable elements of the GNI framework and key insights gleaned from relevant GNI discussions to inform the Special Rapporteur's report, particularly on questions related to how companies can and should anticipate, mitigate, and remedy human rights impacts in conflict scenarios, with a focus on the rights to freedom of expression and privacy.

3. GNI Engagement on Freedom of Expression in Times of Armed Conflict

The GNI framework is grounded in international laws and standards on human rights, as informed by the UNGPs. These frameworks have provided a source of analysis for shared learning, joint policy advocacy, and discussion in the context of GNI assessments about the appropriate roles and responsibilities for ICT companies in conflict scenarios and other sensitive political contexts where rights might face particular threats, including but not limited to such countries as Afghanistan, Ethiopia, Myanmar, and Ukraine.

GNI participants have sought to identify good practice for implementing the principles in such challenging scenarios, including how to implement commitments to human rights due diligence

and impact assessment during and in anticipation of crisis moments. Participants acknowledge the relevance of all applicable laws, including both domestic and international laws, wherever they operate, and seek to implement these commitments in a manner that ensures the safety and liberty of personnel who may be placed at risk.

Russia's invasion of Ukraine drew further attention to the role of ICT companies and services during an inter-state armed conflict, as well as new pressures on ICT companies, including across borders, to restrict access to content and services. The conflict has also added new urgency to a set of considerations and challenges related to the applicability of the GNI framework in the context of international armed conflict where the Law of Armed Conflict (LOAC) applies. In the wake of the invasion, GNI quickly convened internal conversations, as well as external engagements, to foster information sharing, discuss challenges, and generate policy outputs.

Building upon these initial, ad-hoc activities, GNI established a dedicated working group of interested member companies, civil society, academics, and investors to foster understanding of and examine what guidance might be drawn from LOAC by ICT companies operating in these situations. GNI has facilitated the publication of two blog posts to share perspectives on some of the topics that have been discussed through this working group. The first, "Aligning Digital Responses to Armed Conflict with Enduring Value," summarizes initial scoping discussions and sets out the range of topics that the working group hopes to address. The second, "Between a Rock and a Hard Place? ICT Companies, Armed Conflict, and International Law," from GNI academic member Arturo Carrillo outlines key questions and considerations for ICT companies operating in conflict settings, informed by early discussions of the working group.

The insights, which pulled from these discussions and materials, aim to help companies anticipate, prepare for, and prevent negative impacts upon freedom of expression and privacy arising from interstate violence and unrest. GNI will continue to facilitate further conversations along these lines. GNI also invites interested external stakeholders to reach out if they are interested in engaging in these discussions going forward.

4. Questions regarding applicable law and company responsibilities

International human rights law is the primary source of relevant standards and principles for interpreting allowable restrictions on freedom of expression in all contexts, including during times of conflict. Thanks in no small part to the work of the current and previous holders of this mandate, a significant body of interpretative guidance exists explaining the scope and applicability of Articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights (ICCPR).

However, notwithstanding General Comment 11, the recent armed conflict in Ukraine has illustrated the comparative lack of detailed guidance regarding Article 20(1) of the ICCPR, which stipulates that "[a]ny propaganda for war shall be prohibited by law." Relevant questions that have arisen in GNI's internal discussions include the following: How should the terms "propaganda" and "war" be understood, especially as compared to other commonly used terms such as "disinformation" and "armed conflict" respectively? What are the distinctions, if any, regarding how Article 20(1) applies to different states depending on their posture and involvement in the relevant "war"? How does one assess Article 19(3)'s necessity and proportionality tests in the context of an armed conflict? When, if ever, extraterritorial impacts of efforts to restrict freedom of expression taken pursuant Article 20(1) are appropriate and justifiable?

In addition, questions have arisen in our discussions about the relevance and application of certain provisions of LOAC. Examples include the permissibility of "misinformation" as a "ruse of war" as set out in Article 37(2) of Additional Protocol I to the Geneva Conventions, as well as whether information and communication technology infrastructure and services may in some circumstances constitute "objects indispensable to the survival of the civilian population" under the Additional Protocol?

In addition to these questions, are others about how these relevant provisions and principles should be interpreted and used to guide ICT company decision making in conflict contexts. The UNGPs acknowledge that "in situations of armed conflict enterprises should respect the standards of

international humanitarian law,"[1] and John Ruggie, the former UN Special Representative on business and human rights, has explained that in addition to looking to international human rights law, "in situations of conflict, companies themselves ought to be looking to international humanitarian law [IHL] to make sure that they do not find themselves either directly or indirectly contributing to violating IHL provisions or end up complicit in IHL violations."[2] As elaborated in Prof. Carrillo's piece (linked above) where applicable, companies must take on the complex task of navigating the "interplay between the laws of war and human rights law where both are in effect."

5. Relevant provisions of the GNI Principles and Implementation Guidelines

The GNI Principles emphasize 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, ICT companies should avoid, minimize, or otherwise address the adverse impact of government demands, laws, or regulations, and seek ways to honor the principles of internationally recognized human rights to the greatest extent possible. In cases where companies are constrained by national laws, regulations, and policies that are not aligned with international standards, the GNI Principles call on companies to "avoid, minimize, or otherwise address the[ir] adverse impact" and "be able to demonstrate their efforts in this regard.'"[3]

To ensure that companies have systems in place to mitigate these human rights impacts when they occur, the GNI Principles and corresponding Implementation Guidelines stipulate that companies should foster responsible decision making and culture through company policies, procedures and processes. This includes integration of the GNI Principles at all levels of the company, with training for all personnel whose work may touch on significant rights risks, senior-level oversight

[1] UNGPs, Guiding Principle 12, Commentary
[2] "Interview with John Ruggie," *International Review of the Red Cross*, Volume 94 Number 887 Autumn 2012, p. 896, available at: https://international-review.icrc.org/sites/default/files/irrc-887-interview.pdf

[3] See also, "The Operation of the GNI Principles when Local Law Conflicts with Internationally Recognized Human Rights," available at: https://globalnetworkinitiative.org/operating-difficult-jurisdictions/

and accountability of the implementation of the GNI Principles, and procedures for escalation of the most sensitive decisions and significant rights-related risks.

The GNI Principles and Implementation Guidelines also call on companies to "identify circumstances where freedom of expression and privacy may be jeopardized or advanced and integrate these Principles into their decision making in these circumstances," tracking effectiveness in addressing actual or potential adverse impacts that are identified, and communicating how impacts are addressed, consistent with legal obligations. On an ongoing basis, companies conduct human rights due diligence (HRDD) to identify actual and potential rights impacts. Where the potential risks to freedom of expression and privacy are most salient or the potential to advance human rights is greatest, companies also undertake human rights impact assessments (HRIA), engaging with affected stakeholders as part of this process. The Principles also detail scenarios where ongoing HRDD has revealed the need for more detailed HRIA, such as market entry or exit, or designing and introducing new products and services, among other circumstances.

To further our on-going work on HRDD, last year GNI established a dedicated HRDD Working Group that brings together members to discuss and develop guidance for risk assessment, due diligence, and impact assessment in the ICT space. The Working Group is developing tools that will be made available publicly, including through our partnership with Business for Social Responsibility, the Danish Institute for Human Rights, and the UN B-Tech Project on the "Action Coalition on Responsible Tech" organized under the Danish Tech for Democracy Initiative. With respect to HRDD and conflict, GNI appreciates the recent report published by the UN Working Group on business and human rights through its ongoing "business, human rights and conflict-affected regions project" and the recent guide co-developed with UNDP on "The Operation of the GNI Principles when Local Law Conflicts with Internationally Recognized Human Rights," which while not focused on the tech sector specifically nevertheless provide relevant guidance. GNI is also currently supporting additional work being done by GNI NGO participant Just Peace Labs, together with BSR, on developing tools for tech companies that support enhanced due diligence in conflict-affected contexts.

GNI's recommendations for how companies should pursue decision-making around content restriction or providing access to user data in times of conflict remain rooted in this same framework. IHRL standards should always be at the center of how companies shape the design and implementation of their content moderation policies. Situations where LOAC applies might result in the need for companies to take additional considerations into account. For instance, there may be particular risks to consider regarding how to undertake stakeholder engagement without putting such stakeholders at further risk. There are also important considerations around how companies can generate and use leverage vis-à-vis home governments and other non-combatant states. Robust HRDD processes will allow these considerations to be made on a case by case basis, and they therefore should not require changes to the fundamental approaches, systems, and processes companies have established to evaluate the human rights impacts of their products and policies.

6. Key considerations for states responding to conflict

Government decisions concerning freedom of expression in times of conflict must also be guided by IHRL. Maximizing freedom of expression and access to information in conflict zones is crucial. Doing so enables individuals to share and obtain accurate information about conditions in contested areas, coordinate relief efforts, facilitate the documentation of human rights atrocities, and support a variety of other critical functions. In this regard, GNI reiterates its unequivocal condemnation of the actions by the Russian government to restrict access to information and otherwise limit freedom of expression in Ukraine and in Russia as being inconsistent with IHRL.

GNI has also expressed concerns regarding how certain efforts to respond to Russian aggression have resulted in unintended consequences that negatively impact freedom of expression. In March, several major software, hardware, cloud, communications, and internet service providers banned sales and/or suspended services in Russia in part to ensure compliance with sanctions implemented by the U.S. and other governments. GNI signed a letter urging the U.S. Government to issue a General License, "authorizing the provision of services, software, and hardware necessary for personal communications over the internet, and robustly clarifying and disseminating notice of this license to relevant stakeholders." Several months later, the U.S. Office of Foreign Assets Control did just that, helping to mitigate the human rights impacts of these sanctions.

In addition, some attempts to respond to Russian disinformation and propaganda have also raised concerns about their justification under international human rights law on freedom of expression. In March, the E.U. banned Russian news outlets Sputnik and RT due to their role in propagating Russian disinformation about the war in Ukraine. While recognizing the legitimacy of actions to stem the flow of Russian disinformation and propaganda surrounding the war in Ukraine, GNI agrees with the concerns about the ban outlined in freedom of expression Special Mandate holders' Joint Statement on Russia's invasion and the importance of freedom of expression and information, including the danger of the ban being used in/by Russia as a pretext to close independent media outlets in Russia.

GNI acknowledges the legitimate concerns about access to accurate information about the conflict underpinning government responses and continues to grapple with the questions we have previewed in this submission about the lack of consensus and shared understanding on the concept of propaganda in wartime and the potential link to offline violence. However, given the precedential nature of such decisions and the risks of unintended consequences, we reiterate the importance of proceeding with caution, pursuing careful, calibrated responses, and clearly articulating the justification and analysis underpinning such restrictions.

Where states seek to block content, it is paramount that such orders meet the rigorous three-part test of necessity, proportionality, and legality outlined in Article 19(3) of the ICCPR. This means, among other things, they should provide clear, consistent, comprehensive, and timely guidance on precisely what content should be blocked and in what forms/on what types of services it should be blocked. In addition, restrictions that are justified in the context of a conflict should either be time-limited, include periodic revisions to establish if underlying conditions still justify restriction, or be clear about when, how and by whom such determinations will be made.

7. Issues to be considered for further exploration:

- How do conflict scenarios impact different kinds of companies and the services and products they provide, given the distinct degrees of physical presence (both in terms of infrastructure and personnel) required?

- What steps, including collaborative measures, can governments, companies, and other actors take to maintain connectivity in conflict settings?

- Given the often rapidly evolving nature of conflict and the unique nature of each context, what are the proactive steps that governments, companies, and other actors can take to enable rapid and appropriate responses to protect freedom of expression and privacy in the face of quickly deteriorating human rights circumstances?

- What are the cross-border freedom of expression impacts, whether intentional or not, of conflicts and actions taken in response to conflict, and how should these be analyzed and understood through the lens of international human rights law?

- In cases requiring the legal limitation of fundamental rights to freedom of expression, what kind of legal obligations and corresponding liability should be imposed on companies, considering the different types of products and services they provide?

8. Conclusion

GNI welcomes the opportunity to engage with the Special Rapporteur, her staff, and other stakeholders to continue exploring and creating guidance for responsible conduct by governments, companies, and others in times of armed conflict and other disturbances. We look forward to the Special Rapporteur's report and her future work on these topics.