April 1, 2016

Office of the High Commissioner for Human Rights
United Nations Office at Geneva
CH-1211 Geneva 10
Switzerland

RE: Input to the report on how protecting and promoting human rights contribute to preventing and countering violent extremism

The Global Network Initiative welcomes the opportunity to provide input to the report of the Office of the UN High Commissioner for Human Rights regarding human rights and preventing and countering violent extremism, pursuant to resolution 30/15 of the Human Rights Council.

The Global Network Initiative is an international, multi-stakeholder collaboration between information and communications technology (ICT) companies, civil society organizations, investors, and academics. Formed in 2008, our mission is to promote human rights by creating a global standard for companies that supports responsible decision-making, and by being a leading voice in policy debates to advance freedom of expression and privacy rights in the ICT sector. By implementing the GNI Principles, ICT companies worldwide can fulfill their responsibility to respect human rights in accordance with the UN Guiding Principles on Business and Human Rights.

In July of 2015, the GNI launched a policy dialogue aimed at exploring key questions and considerations to inform debate and foster collaboration on the issue of extremist content online and the ICT sector in a multi-stakeholder setting.1 The GNI has held closed roundtable discussions and public events, and we have participated in the recent meetings of the UN Counter-Terrorism Committee devoted to this topic.

The GNI began its dialogue by acknowledging the legitimate national security and law enforcement obligations of governments. At the same time, it is concerned that the rush to adopt laws and policies that increase government pressure or requirements on companies to restrict or remove content may have serious consequences for freedom of expression and may not be effective in countering violent extremism and stemming recruitment by organizations such as ISIL. The GNI would like to share four principle lessons that have emerged from this dialogue thus far.

---


1) Strategies that focus on the restriction of online content should be consistent with the protection of the right to freedom of expression

The GNI has observed that in pursuit of the legitimate aim of protecting national security, some states have sought to impose greater restrictions on online communications. When laws and policies that involve the restriction of content deemed to be extremist or terrorist are adopted, the GNI urges states to ensure that they are consistent with the fundamental right to freedom of expression. These laws and policies should be debated and adopted in a multi-stakeholder setting, and they should meet the tests of legality, necessity, proportionality required by Article 19 of the International Covenant on Civil and Political Rights (ICCPR).

A. Restrictions on the right to freedom of expression often appear to be inconsistent with the principle of legality

The GNI is concerned that the adoption of broad laws prohibiting extremist content and the promotion of terrorism may fail to meet the standard contained in Article 19 of the ICCPR. In order to comply with its principle of legality, a law “must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly . . . A law may not confer unfettered discretion for the restriction of freedom of expression on those charged with its execution.”

Furthermore, the Human Rights Committee has stated that

[s]uch offenses as “encouragement of terrorism” and “extremist activity” as well as offences of “praising”, “glorifying”, or “justifying” terrorism, should be clearly defined to ensure that they do not lead to unnecessary or disproportionate interference with freedom of expression.3

Resolutions of the UN Security Council that call on states to prohibit incitement to terrorism and to collaborate in their efforts to prevent the use of technology to commit terrorist acts have also emphasized that state action must be consistent with international human rights law.4

The GNI acknowledges the complexity of these issues and recalls that there continues to be no internationally agreed upon definition of terrorism. Across the world, counterterrorism laws have led to the criminalization of speech in political contexts. For example, a comedian was convicted under counterterrorist laws in France for having posted the statement “I feel like Charlie Coulibaly” on his Facebook page shortly after the terrorist attacks of January 2015.5 Recently, puppeteers were arrested

---

3 CCPR/C/GC/34, para. 46.
5 BBC. Dieudonne guilty of condoning terrorism with Charlie Hebdo comment, March 18, 2015.
in Spain under counterterrorism laws for a satirical performance which had criticized the application of these laws.\textsuperscript{6}

Separately, private companies retain discretion to set content policies under terms of service, which reflect their brand and nature of their services. Policies will vary depending on the different nature and type of services provided. The GNI has noted reports of increased action by some governments to influence the content policies of ICT companies and to use these policies to secure the removal of content through informal mechanisms, wholly outside the legal process. This trend risks setting precedents for extra-judicial government censorship without adequate transparency for users and the public at large (although many companies report such removal requests in their respective transparency reports). It is the practice in the United Kingdom, for example, for the police to refer alleged terrorist content to companies for removal as violations of company content policies, and Europol aims to extend this approach via the creation of an Internet Referral Unit that would coordinate referrals across the EU.

**B. Restrictions on the right to freedom of expression may be inconsistent with the principles of necessity and proportionality**

The GNI is concerned that the restriction of online content often does not conform to the tests of necessity and proportionality required by Article 19. As the Human Rights Committee has stated, a restrictive measure “violates the test of necessity if the protection could be achieved in other ways that do not restrict freedom of expression.”\textsuperscript{7} In order to be proportionate, restrictive measures “must be the least intrusive instrument amongst those which might achieve their protective function,” and it is incumbent on the State to “demonstrate in specific and individualized fashion the precise nature of the threat, and the necessity and proportionality of the specific action taken, in particular by establishing a direct and immediate connection between the expression and the threat.”\textsuperscript{8}

One troubling example of government actions that appear inconsistent with the tests of necessity and proportionality is the blocking of an entire service, such as YouTube, based on the conclusion that specific material on that site violates a State’s counterterrorism laws.\textsuperscript{9} Participants in our dialogue have questioned whether this approach is likely to be effective in countering violent extremism and whether it may reduce opportunities for the creation and dissemination of alternative messages that

---


\textsuperscript{7} CCPR/C/GC/34 para. 33.

\textsuperscript{8} CCPR/C/GC/34 para. 34-35.

discourage violence. The GNI encourages states to examine the necessity and proportionality of policies aimed at restricting online content, taking into account available evidence and research in this area.

2) In order to be consistent with international human rights standards, the liability of Internet intermediaries for third party content should be limited

In the course of the debate on extremist content online, state authorities have proposed that intermediary service providers could bear criminal responsibility or civil liability for providing access to or transmitting user-generated content related to terrorism, regardless of whether they have intervened in that content. Authorities have also proposed that intermediaries be required to monitor third-party content that is hosted on their sites. For example, the most recent draft of the Prevention of Electronic Crimes Bill in Pakistan would use broad language to impose penalties on those who prepare or disseminate information online with the intent to “glorify an offence or the person accused or convicted of a crime and support terrorism or activities of proscribed organizations.”

According to a recent resolution of the European Parliament,

Member States should consider legal actions, including criminal prosecutions, against internet and social media companies and service providers which refuse to comply with an administrative or judicial request to delete illegal content or content praising terrorism on their internet platforms.

In the United States, legislation has been introduced that would require ICT companies to report terrorist activity to the authorities under certain circumstances and at least one civil action has been filed against Twitter alleging that it has provided material support to ISIL by allowing it to use its service.

The GNI has maintained that policies creating liability for intermediaries on the basis of content sent or created by users chill freedom of expression by incentivizing carriers to restrict the use of their services for any content that could be considered controversial, or to limit the pseudonymous or anonymous use of these services. The UN and regional rapporteurs for freedom of expression have also stated that imposing liability on online intermediaries for third-party content when they have not intervened in the content or refused to obey a court order to remove it is inconsistent with the protection of the right to freedom of expression online. Additionally, the Manila

11 European Parliament resolution of 25 November 2015 on the Prevention of radicalisation and recruitment of European citizens by terrorist organisations, para. 16 (2015/2063(INI)).
12 S.2732, Requiring Reporting of Online Terrorist Activity Act, December 8, 2015 (United States).
Principles on Intermediary Liability indicate that Internet intermediaries must not face strict liability for hosting unlawful third-party content and should not be required to monitor content proactively.\(^{15}\) Instead, states should pursue legal action related to unlawful content against the author of such content.\(^{16}\)

3) State actions should not penalize the creation and dissemination of alternative messages

The role of state authorities in creating and disseminating messages that discourage radicalization and debunk extremist propaganda has been debated in many fora, including roundtable discussions and public events hosted by the GNI. While this is a matter for discussion among a broad group of experts and policymakers, the GNI has identified some preliminary considerations. First, states should ensure that their regulatory frameworks do not penalize or undermine Internet users’ right to freedom of expression, which in turn undermines the ability of private actors to develop and disseminate alternative messages that are authentic and credible within their own communities.

Second, states should ensure that journalists and media outlets in particular are not penalized for carrying out their activities, including reporting on terrorist groups and informing the public about acts of terrorism.\(^{17}\) Third, states should not compel speech on the part of private actors as part of their efforts to protect national security or public order. Non-state actors should have the freedom to experiment with different tools for addressing extremist content online.

4) Transparency and the multi-stakeholder approach to policymaking

The GNI has advocated for states to take steps to be more transparent about the laws and practices that govern the restriction of online content in general. The GNI has encouraged states to disclose the laws that authorize orders to restrict content and the interpretations of those laws, as well as which government agencies are legally authorized to order content restriction, the oversight mechanisms that are in place, and


\(^{16}\) A/HRC/17/27 para. 43.

\(^{17}\) See Courtney Radsch, *One year after Charlie Hebdo, will press freedom become victim of war on terror?* January 2016, available at: 
the mechanisms for redress that victims of unlawful censorship may pursue. States should not prohibit companies from disclosing the number of requests that they receive to restrict content. Similar measures of transparency should govern state action when authorities use Internet referral units or methods that are developed for a service’s users to obtain the removal of content.

Finally, we urge governments and intergovernmental organizations to take a multi-stakeholder approach when debating laws and policies that impact the freedom of expression and privacy of Internet users globally and to ensure that these are subject to public debate.¹⁸