GLOBAL NETWORK INITIATIVE

Extremist Content and the ICT Sector

A Global Network Initiative Policy Brief

November 2016

Introduction

The role of information and communication technology (ICT) companies in responding to alleged terrorist or extremist content has become one of the most challenging issues for freedom of expression and privacy online.[1] In July 2015, GNI launched a policy dialogue to explore key questions and considerations concerning government efforts to restrict online content with the aim of protecting public safety, and to discuss the human rights implications of such government actions.[2]

As part of this dialogue, GNI has convened a series of roundtable discussions, bringing together its academic, civil society, investor, and company participants with other experts and representatives from governments and international organizations. The roundtables—held under the Chatham House rule—were hosted in London in October 2015, Washington, DC, in February 2016, San Francisco in March 2016, and Brussels in June 2016. In addition, GNI staff and participants have engaged in meetings of the UN Counter-Terrorism Committee and in public panel discussions on this subject. See Appendix I for a complete list of events.

Based on these consultations and extensive deliberations among our participants, GNI has developed a set of recommendations for governments and companies, set out in detail in this document. They are inspired by the GNI Principles and Implementation Guidelines, and informed by relevant international human rights standards as laid out in the Joint Declaration on Freedom of Expression and countering violent extremism and the UN Guiding Principles on Business and Human Rights.[3] Below is a summary of GNI's recommendations, followed by the complete recommendations with respect to: 1) governments; 2) companies; and 3) government referral of alleged terms of service violations to companies.

---

[1] This document uses the term "extremist content" to refer to material that is allegedly linked to terrorism, including material that is alleged to radicalize individuals, recruit funds for terrorist organizations, and/or encourage individuals to commit violent acts or to become foreign terrorist fighters. The GNI recognizes that there are no internationally agreed upon definitions of "extremism" or "terrorism." Across the world anti-terrorist laws have been used to harass, intimidate and imprison individuals - including journalists, bloggers, artists, lawyers, and human rights defenders.

[2] Extremist Content and the ICT Sector – Launching a GNI Policy Dialogue, available at http://globalnetworkinitiative.org/news/extremist-content-and-ict-sector-launching-gni-policy-dialogue.

[3] The GNI Principles and Implementation Guidelines are available at: http://globalnetworkinitiative.org/corecommitments/index.php. The Joint Declaration on Freedom of Expression and countering violent extremism, by UN Special Rapporteur on freedom of opinion and expression, David Kaye, Representative on Freedom of the Media of the Organization for Security and Co-operation in Europe (OSCE), Dunja Mijatovic, Special Rapporteur on Freedom of Expression of the Inter-American Commission on Human Rights, Edison Lanza, and Special Rapporteur on Freedom of Expression and Access to Information of the African Commission on Human and Peoples' Rights (ACHPR), Pansy Tlakula, is available at: http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=19915&LangID=E.

Summary of Recommendations

- Governments must protect and respect human rights when developing, implementing, and enforcing laws and policies meant to address extremist content online.
- Government legal demands to restrict content for the purpose of protecting public safety must be pursuant to the rule of law. They should respect and protect freedom of expression and privacy, and be directed at creators of content, rather than intermediaries, whenever possible.
- Governments must not impose liability—directly or indirectly—on intermediaries on the basis of content sent or created by third parties. Intermediaries must not be required to monitor third-party content that they host or transmit.
- Governments should not pressure companies to change their terms of service (TOS). Companies develop TOS in order to deliver user experiences that are appropriate for the nature or type of service, and the user community of the service.
- When governments refer content to companies for removal under companies' TOS, governments should guard against the risks that such referrals may set precedents for extra-judicial government censorship without adequate access to remedy, accountability, or transparency for users and the public. If governments make such referrals, they should be transparent about, and accountable for, such referrals.
- Companies should be transparent with their users when required by governments to remove or restrict content, unless prohibited by law.

I) GNI Recommendations for Governments

GNI acknowledges the legitimate national security and law enforcement obligations of governments. At the same time, GNI is concerned about laws and policies that may have serious consequences for human rights without necessarily providing effective strategies to counter violent extremism or stem recruitment by terrorist organizations. This includes the adoption of laws and policies that inadequately protect rights to free expression and privacy, as well as the application of government pressure on companies to restrict or remove content outside the legal process.

Consistency with international human rights norms – When passing laws and adopting policies meant to address extremist content online, governments must fulfill their duty to protect the right to freedom of opinion and expression, which includes the freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers. This is a fundamental right enshrined in Article 19 of the International Covenant on Civil and Political Rights, as well as in regional human rights instruments.

Necessary and proportionate means – Restrictions on the right to freedom of expression must be established in a law that is clear and precise, must pursue a legitimate aim, and must be a necessary and proportionate means of achieving that aim.[4] Governments must ensure that laws and policies prohibiting incitement to terrorism use clear and precise language. They should only target unlawful speech that is intended to incite the commission of a terrorist offense and that causes a danger that a terrorist offense or violent act may be committed.[5] Government restrictions should be content-specific and should not target entire sites, platforms or services.[6] These laws and policies must not lead to unnecessary or disproportionate interference with freedom of expression, nor may they target political speech. Government legal demands to restrict content for the purpose of protecting public safety must be pursuant to and governed by the rule of law.

Alternative messages – Governments must ensure that counterterrorism laws and policies do not undermine the development and dissemination of messages by private actors that discuss, debate, or report on terrorist activities.

- Laws and policies must distinguish between messages that aim to incite terrorist acts and those that discuss, debate or report on them.
- Journalists and media outlets must not be penalized for reporting or providing commentary about terrorist groups, or for informing the public about acts of terrorism.
- Governments must not compel speech or dissemination of speech by private actors as part of their efforts to protect national security or public order.
- Governments should not prohibit the use of encryption technologies, compel the weakening of security systems, nor seek to subvert digital security standards in other ways. Such technologies preserve speakers' abilities to communicate alternative messages.

Intermediary liability – Governments must not impose liability on intermediaries on the basis of content sent or created by third parties. Intermediaries must not be required to monitor third-party content that they host or transmit. Liability and monitoring requirements are likely to cause intermediaries to remove content even

[4] See CCPR/C/GC/34, paras. 21 *et seq*; European Court of Human Rights, *Case of The Sunday Times v. United Kingdom (No. 1),* App. No. 6538/74 (26 April 1979), paras. 45-59; Inter-Am. Ct. H.R., *Herrera Ulloa v. Costa Rica,* Series C No. 107 (2 July 2004), paras. 120-23; African Commission on Human and Peoples' Rights, *Media Rights Agenda and others v. Nigeria*, Comm. Nos. 105/93, 128/94, 130/94 and 152/96 (1998), paras. 65-70.

[5] See, e.g., Report of the special rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, A/HRC/16/51 (22 December 2010), para. 31; Report of the special rapporteur for the promotion and protection of the right to freedom of opinion and expression, A/66/290 (10 August 2011), para. 34; Convention on the Prevention of Terrorism, CETS No. 196, 16 May 2005, Article 5.

[6] See CCPR/C/GC/34, para 43.

when the removal may not be legally required.[7] Instead, when necessary and proportionate, governments should pursue legal action related to specific, alleged unlawful content against the creator of the content.

Transparency – Governments must make publicly available the laws, legal interpretations and policies authorizing content restriction. Governments must also disclose information about the agencies that are legally permitted to order restrictions, the substantive standards for any restrictions, and the due process and oversight mechanisms involved in content restriction.

- Governments should regularly and publicly report, at a minimum, the aggregate numbers of requests and/or legal orders made to companies to restrict content and the number of users impacted by these requests.
- Governments must not prohibit companies from disclosing, in any way, the number of requests and/or legal orders to restrict content that they receive, and how the company responded to the request.
- Governments must not prohibit companies from reporting on companies' own efforts to restrict extremist content.

Multi-stakeholder policy development – At the state and international level, laws, standards and policies that affect the rights to freedom of expression and privacy must be developed in an open, transparent, participatory process involving all relevant stakeholders, and must be clearly described in publicly available documents.

Remedy – Governments must ensure that alleged violations of the right to freedom of expression and privacy are investigated, and that effective remedies are available when such violations have occurred. Governments must disclose publicly the mechanisms for redress that victims of unlawful government censorship may pursue.

II) GNI Recommendations for Companies

Many companies, including GNI participants, have taken a variety of steps to address extremist content that is accessible through their services. Private companies retain discretion to set content policies under TOS which reflect their brand and the particular services they provide. Policies will vary depending on the nature and type of services provided: e.g., hosted content, communication services, search engine services, etc.

[7] The imposition of intermediary liability is likely to incentivize companies to restrict the use of their services for any content that could be considered controversial, preventing the creation of content as well as increasing the likelihood of its removal. Moreover, imposing monitoring requirements may also threaten the privacy rights of users who are not suspected of any crime.

Human rights principles – GNI has developed a set of Principles and Implementation Guidelines through a multi-stakeholder process to guide company action when government demands, laws and regulations restrict content, limit freedom of expression, infringe on privacy, or otherwise limit access to information and ideas in a manner inconsistent with internationally recognized laws and standards for human rights.

ICT companies should respect the rights to freedom of expression and privacy by committing to the GNI Principles.

When required by governments to restrict or remove content, companies should:

- Require that governments follow established domestic legal processes when they make demands that restrict freedom of expression.
- Interpret government restrictions and demands, as well as the governmental authority's jurisdiction, so as to minimize the negative effect on freedom of expression.
- Seek clarification or modification from authorized officials when government restrictions appear overbroad, are not required by domestic law, or appear inconsistent with international human rights laws and standards on freedom of expression.

Transparency – ICT companies should operate in a transparent manner with their users and the public when required by governments to remove or restrict content, and should encourage governments to introduce transparency reporting.

III) Recommendations for Government Referral of Alleged TOS Violations to Companies

Some governments have established new mechanisms and structures that are intended to use the content policies of ICT companies to request the removal of content through the companies' own mechanisms for reporting alleged violation of companies' TOS, wholly outside the legal process. Some stakeholders are concerned that this type of government referral of content could set precedents for extra-judicial government censorship without adequate access to remedy, accountability, or transparency for users and the public.

Of particular concern are requests for TOS enforcement made by governments anonymously through user-facing reporting tools, where companies may be unable to identify the request as coming from a government agency. People acting on behalf of government authorities should identify themselves as government representatives for any requests. Companies develop and enforce their TOS for business reasons, such as delivering user experiences that are appropriate for the nature or type of service they provide and/or their user community. TOS enforcement decisions by GNI member

companies do not change based on whether the allegedly inappropriate content is referred to the companies by governments or by any other third party.

Several governments already engage in content referrals in an effort to counter violent extremism online. Governments should adopt additional safeguards to ensure such referrals do not circumvent legal procedures and do not have unintended consequences. In this context and in each instance, governments should be clear and transparent as to whether they are submitting to a company a report or referral of an alleged terms of service violation or issuing a legal order requiring content removal or restriction.

Formal legal process – Governments must use formally established legal procedures when they demand the restriction of content by ICT companies.

- Governments must use formal legal process to send orders to remove content, rather than consumer-facing reporting tools, so that legal orders can be recorded as such.
- When Governments make requests to companies to remove content that allegedly violates TOS, outside of regular legal processes, governments must be transparent about and accountable for such referrals. Governments must not compel ICT companies to change how they develop and enforce their TOS.

Transparency – Governments and ICT companies should be transparent about TOS-based referrals, and should seek to disclose relevant information as appropriate. As noted above, governments should regularly and publicly report, at a minimum, the aggregate numbers of requests made to companies to restrict content and the number of users impacted by these requests. When governments self-identify in the course of reporting alleged violations of terms of service to companies, companies should be transparent about such referrals. For example, companies can include these referrals as government requests for content removal in their transparency reports.

Remedy – ICT companies should provide mechanisms for remedy that allow people who believe their account has been suspended erroneously as a result of these referrals to seek reinstatement of their account. Government must provide users with access to effective remedy relating to government referral of alleged violations of companies' terms of service.

Multi-stakeholder efforts, including companies, NGOs, academic institutions, and socially responsible investors, should engage in dialogues with governments about the GNI Principles and to encourage governments to adopt the recommendations in this paper.

Looking Ahead

It is critical that governments and companies engage in dialogue with a wide variety of global stakeholders as they develop policies and practices regarding extremist content. GNI will continue to actively engage on this topic in future learning and policy efforts.

Individually and collectively, GNI and its members will use these recommendations as the basis for future public policy engagement and shared learning. For example, GNI has joined the advisory board of the UN Counter-Terrorism Executive Directorate joint project on private sector engagement in responding to terrorists' use of ICTs.[8]

If you are interested in engaging with GNI on extremist content or other policy issues, please contact us at info@globalnetworkinitiative.org or visit our website.

[8] See http://www.un.org/en/sc/ctc/news/2016-04-20_CTED_ICT4Peace.html.

Appendix I: Consultations and Events

New York (April 24, 2015): GNI staff attended a workshop on collaboration to counter terrorist exploitation of ICTs organized by the UN CTED and NYU's School of Professional Studies/Center for Global Affairs.

Madrid (July 28-29, 2015): GNI presented at an expert session prior to a special meeting of the UN Counter-Terrorism Committee on how to stem the flow of foreign terrorist fighters, and a closed roundtable with UN, EU, and government stakeholders.

New York (September 14, 2015): GNI Executive Director Judith Lichtenberg addressed the United Nations Counter-Terrorism Committee on the multi-stakeholder approach to best-practice regulation of incitement and violent extremism online.

London (October 16, 2015): GNI and the Center for Democracy & Technology hosted a closed roundtable session on the regulation of extremist content online.

Sao Paulo (November 12, 2015): GNI spoke at an Internet Governance Forum workshop on Dangerous Speech, and at a UNESCO workshop on hate speech and radicalization.

Palo Alto (December 2, 2015): GNI and the Stanford Center for Internet & Society hosted a public learning day featuring a panel discussion on extremist content online.

New York (December 16-17, 2015): GNI participated in a meeting of the UN CTED on "Preventing Terrorists from Exploiting the Internet and Social Media Recruit Terrorists and Incite Terrorist Acts, While Respecting Human Rights and Fundamental Freedoms"

Washington, DC (February 17, 2016): GNI and the American Society of International Law hosted a closed roundtable session on the regulation of extremist content online.

Austin (March 15, 2016): GNI spoke at SXSW Interactive at a panel on "How to Fight ISIS Without Breaking the Internet."

Washington, DC (March 23, 2016): GNI spoke at George Washington University at a policy forum, entitled "What are the responsibilities of tech companies in an age of international Terrorism?"

San Francisco (March 30, 2016): GNI organized a session at RightsCon on combating terrorism online, featuring an update from our Policy Dialogue.

Geneva (April 7, 2016): GNI addressed the Geneva Conference on Preventing Violent Extremism – The Way Forward, organized by the UN and the Government of Switzerland.

Brussels (June 2, 2016): GNI and the Telecommunications Industry Dialogue hosted a closed roundtable session that included extremist content.