Extremist Content and the ICT Sector

Launching a GNI Policy Dialogue

July 2015

Protecting and Advancing Freedom of Expression and Privacy in Information and Communications Technologies

In the months since the terrorist attacks in Paris and Copenhagen, the debate over the role of information and communication technology (ICT) companies in removing alleged terrorist or extremist online content has accelerated significantly.

The Global Network Initiative (GNI), while acknowledging the legitimate national security and law enforcement obligations of governments, 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 ISIS.

These issues are complex. There continues to be no internationally agreed upon definition of terrorism. [1] Across the world anti-terrorist laws have been used to imprison journalists, bloggers, and human rights defenders.[2]

International human rights law provides specific conditions under which States can act to restrict freedom of expression. These include that any restriction must be provided for in law and done in pursuit of a legitimate aim.[3] Any measures adopted must also be proportionate to the perceived harm and necessary to countering it. In addition, there are procedural safeguards that must accompany government efforts to restrict freedom of expression, including review by an independent authority and the availability of remedy.[4] National laws, however, differ significantly as to what content is deemed unlawful and in what contexts. For example, some states have criminalized the publication of content that promotes, incentivizes or glorifies acts of terrorism in a bid to counter propaganda messages and recruitment, particularly of foreign fighters.

Currently, processes to identify illegal content vary among countries. Some countries have recently legislated to criminalize certain extremist content and assign responsibility for assessing legality to an independent, and publicly accountable body. Other countries empower law enforcement officers to assess content and notify providers individually of suspect content.

---

[1] See Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin (22 December 20120), p. 13, http://www.refworld.org/docid/4e0c2ace15.html.
[2] For example, see the case of the Zone 9 bloggers in Ethiopia. See Jacey Fortin, "Conflating terrorism and journalism in Ethiopia," Attacks on the Press (2015 edition), Committee to Protect Journalists, https://cpj.org/2015/04/attacks-on-the-press-conflating-terrorism-and-journalism-in-ethiopia.php.
[3] See Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue (16 May 2011), p. 8, http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.
[4] *Id.*

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. For example, hosted content is different from referral content, such as search engine results, which are an index or catalog of the available information on the web. There is 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.[5] Finally, the differing criminal thresholds in national laws add a further layer of complexity, as content hosted in one country can be widely available in another where it could be deemed criminal.

GNI encourages governments and intergovernmental organizations to consult broadly with affected stakeholders, experts and the public to address and resolve important questions as they consider these measures. As part of GNI's shared learning and policy engagement, we will focus on this issue during the coming months, and develop a policy and learning agenda that brings together our participants to explore the following key questions.

Key questions and considerations

1) How have government efforts to restrict online content been implemented in the past?

- What are the range of laws and policies employed by governments to pursue removal of content?
- Are there practices or examples of such governmental measures that can be compiled, analyzed and evaluated for guidance?
- How do governments deal with tensions between legal thresholds in different countries?

2) How should governments assess whether specific content poses sufficient threat to national security or public safety to warrant a necessary and proportionate restriction?

- What types of content may be legitimately restricted by governments?
- Are there particular norms or principles that should be required when governments are considering any such restrictions? What evidence base (in terms of harm) is required?

[5] Vikram Dodd, "Europol web unit to hunt extremists behind Isis social media propaganda," *The Guardian*, 21 June 2015, http://www.theguardian.com/world/2015/jun/21/europol-internet-unit-track-down-extremists-isis-social-media-propaganda.

- How should the boundaries between commentary on ideology and extremist content be handled?

- How should context be taken into account when assessing content (e.g.: when extremist content is used in counter-speech or journalism)?

3) What would constitute a necessary and proportionate government restriction or defensive measure that is consistent with international human rights laws and standards and the rule of law?

- What are the legal, ethical and efficacy considerations of governments employing (or forcing companies to employ) automated methods of identifying such content?

- What are the implications of governmental efforts to increase the removal of extremist content given the size and scale of social networks and digital communications tools?

- What level of transparency should there be? What rights of redress should individuals and organizations have?

4) What are substantive criteria and minimum due process protections, including an independent impartial authority, appropriate to review and adjudicate government-mandated content restrictions?

- What should be the respective roles of government agencies, judicial authorities, ICT companies, and their users in removing illegal content?

Call for Collaboration

GNI and its participants will explore these questions through research and shared learning during the second half of 2015. We will seek to bring together diverse viewpoints from government, international organizations, ICT companies, academics, investors, and civil society. Our aim is to identify points of consensus, areas for further research, and policy approaches that protect both security and human rights.

Specifically, GNI will:

- Convene experts to address this issue virtually and in person

- Commission research to address these issues, for publication by December 2015

Please contact us at info@globalnetworkinitiative.org if you are interested in engaging with us on this topic.