

GNI Talking Points at the UN Counter-Terrorism Meeting in Madrid, July 27-29

TALKING POINTS

About GNI (2-3 minutes)

GNI is a multi-stakeholder initiative that brings together ICT companies with human rights groups, investors, and academics to forge a common approach to free expression and privacy online.

GNI's principles are based on internationally recognized laws and standards for human rights set in the Universal Declaration of Human Rights ("UDHR"), the International Covenant on Civil and Political Rights ("ICCPR") and the International Covenant on Economic, Social and Cultural Rights ("ICESCR").

Our principles and implementation guidelines guide responsible company decision-making when facing requests from governments around the world that could impact the freedom of expression and privacy rights of users. Our accountability process uses independent assessment to verify that companies are implementing the principles.

ICT companies worldwide can use the GNI's principles, guidelines and tools to assess human rights risk when entering or leaving a market or when designing and introducing new technologies, products or services. By working together with human rights groups, investors and academics, ICT companies can manage human rights challenges, maintain credibility and support the privacy and freedom of expression rights of their users. Currently, GNI has six company members: Microsoft, Facebook, Google, Yahoo!, LinkedIn, and ProCera Networks.

Governments' Initiatives (5-6 minutes)

Increased public safety and national security concerns associated with online activities of terrorist groups have led to a widespread push to put requirements on ICT companies, which are often perceived as natural point of control for illegal content.

GNI acknowledges the legitimate national security and law enforcement interests of governments; however, GNI is concerned that the rush to adopt laws and policies that increase obligations of ICT companies to monitor and restrict terrorist activities pose serious consequences for freedom of expression and privacy and create challenges for ICT companies to uphold GNI principles.

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

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. 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.

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.

There is also 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. 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.

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.

Among the range of anti-terrorist initiatives and subsequent requirements on ICT companies, many have the potential to pose risks to human rights. Among them are:

- Anti-terrorist laws that grant excessive powers to states and law enforcement to limit speech by placing legal obligations on ICT companies to monitor and/or censor content, build backdoors into their products, change their infrastructure, record communications, etc.
- Requirements that ICT companies block allegedly terrorist material without a court order and public accountability.
- Establishment of vague, affirmative obligations for ICT companies to notify governments of potential “terrorist” content.
- Pressure on ICT companies to change their terms of service to ensure removal of certain content.

- Action taken against ICT companies, such as bans, fines and prosecution, for failing to comply with overbroad anti-terrorist laws to remove content.
- Holding ICT companies liable for hosting and indexing content that could qualify as “extremist”.

Human Rights Vulnerabilities (1-2 minutes)

GNI believes that it is detrimental to freedom of expression and privacy to place liability on ICT companies on the basis of extremist content sent or produced by users. Such liability effectively requires companies to engage in self-censorship and prior restraints on speech, particularly in jurisdictions where definitions of illegal content are vague and overbroad and can be used to imprison journalists, bloggers, human rights defenders for simply doing their jobs, and users for simply speaking out their minds online. These obligations would also require companies to routinely disregard the privacy of their users in search of “extremist” content. Such regulations would not only be difficult to enforce and harmful to civil liberties, but they would also give a pretext for repressive governments to adopt similar tools with the goal of cracking down on dissent. Even governmental efforts to influence companies’ in-house policies to secure content removal through informal mechanisms risk setting precedents for extra-judicial government censorship.

Recommendation (5-6 minutes)

Given the potential for unintended consequences such as facilitating human rights violations by some governments, there is a need for clearer articulation of the relationship between online extremism, company practices, and existing regulations before determining whether additional regulation is the optimal means of addressing online terrorist activities.

There is also an urgent need to understand the role of counter speech in challenging terrorist ideology. Unrestricted campaigns and discussions of terrorism related subjects by the civil society and the media can offer alternative narratives, potentially serving as a useful counter-terrorism strategy.

Ultimately, efforts to identify terrorist threats and thwart them should take place within the rule of law, the international standards of human rights, and should not interfere with company's responsibility to respect freedom of expression and privacy rights of their users. Any restrictions that do meet such conditions should further be carried out in a manner that demonstrates commitment by governments as well as companies to maximize transparency and accountability.

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.

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?
 - 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?

In an attempt to bring together a broad range of stakeholders, GNI and Center for Democracy & Technology (CDT) will be setting up an expert meeting on extremist content on October 16, 2015 with a selection of companies, NGOs, experts and officials from the security and law enforcement community. The goal of the meeting is to assess relevant issues and identify effective and proportionate solutions. We encourage NGOs and authorities to join the meeting.