GLOBAL NETWORK INITIATIVE

Right Honorable Jacinda Ardern
Prime Minister of New Zealand

May 14, 2019

Honorable Emmanuel Macron
President of the French Republic

Dear Prime Minister Ardern and President Macron,

On behalf of our 62 globally diverse academic, civil society, company, and investor members, the Global Network Initiative (GNI) thanks you for the invitation to participate in the May 14 "Voices for Action" event in Paris. Although we are unable to attend and still have not received the official text of the *Christchurch Call*, we nevertheless would like to take this opportunity to provide some suggestions ahead of these meetings based on our experience fostering constructive engagement between policy makers and our globally diverse membership of information and communication technology (ICT) companies, human rights and media freedom organizations, academics, and investors.

Given the importance of the *Christchurch Call* and its potential ramifications for civil society, journalists, technology platforms, and internet users around the world, it is essential that this initiative be conducted in an open and inclusive manner. We have heard from many leading organizations that the late notice and the lack of an opportunity to participate in the shaping of the text of the *Christchurch Call* have presented serious barriers to their effective engagement. The unfortunate exclusion of civil society from the 15 May meetings between governments and companies further undermines confidence in this process.

As we recently recommended to the UN High Level Panel on Digital Cooperation, diversity and inclusion are key ingredients in meaningful engagement of participants, a core component of effective multi-stakeholder initiatives. For cross-border and universal issues, such as those in the digital realm, a truly diverse group makes fewer assumptions, increases the robustness of policy positions and advocacy strategies, and anticipates and minimizes otherwise unforeseen harms or challenges. Taking active steps to ensure that all participants have the opportunities, resources, and tools available to help them succeed within the cooperative initiative is essential to this approach.

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, as seen most recently with the horrific murders in Christchurch. 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. As part of this multi-year dialogue, GNI 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.

Based on these roundtables and our engagements with the UN Counter Terrorism Committee and others, GNI developed a set of recommendations for governments and companies, set out in detail in our *Extremist Content and the ICT Sector* policy brief.[1] 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. We have appended the key recommendations from the policy brief to this letter.

Substantively, we want to underscore the importance of framing the *Christchurch Call* in international human rights language. Through ten years as an organization, GNI has found that shared respect for human rights provides a foundation upon which to build consensus among diverse and varied stakeholders. GNI, the only multi-stakeholder membership organization focused on the ICT sector, has used this approach to build trust and cooperation among diverse stakeholders, produce important research on topics of mutual interest, and advocate collectively for freedom of expression and privacy in countries across the world. GNI's approach is informed by the UN Guiding Principles on Business and Human Rights, which articulate the obligations of both governments and companies to protect, respect, promote, and support human rights.

Human rights, such as freedom of expression, non-discrimination, and diversity of thought, represent the very values that terrorist ideologies attack and seek to suppress. It is therefore imperative that we take great care to ensure that our efforts to counter terrorism avoid infringing on those very rights. 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 is eager to coordinate with your governments on this initiative. Please direct future communications to jlichtenberg@globalnetworkinitiative.org.

Sincerely,

Judith Lichtenberg
Executive Director
Global Network Initiative

[1] Extremist Content and the ICT Sector: A Global Network Initiative Policy Brief, November 2016, available at: https://globalnetworkinitiative.org/wp-content/uploads/2016/12/Extremist-Content-and-ICT-Sector.pdf

APPENDIX: Recommendations from GNI's Extremist Content and the ICT Sector Policy Brief:

Recommendations for governments:

- **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.
- **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.
- **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.

Recommendations related to transparency:

- **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.**
- **Companies should be transparent with their users when required by governments to remove or restrict content, unless prohibited by law.**

Recommendations for companies:

- **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.**