December 20, 2017

David Kaye
Special Rapporteur on the right to freedom of opinion and expression
Office of the United Nations High Commissioner for Human Rights
Geneva, Switzerland
freedex@ohchr.org

RE: Submission on Content Regulation in the Digital Age

The Global Network Initiative (GNI) welcomes the opportunity to provide input to the Special Rapporteur's study on content regulation in the digital age.

GNI is a unique multi-stakeholder forum bringing together Information and Communications Technology (ICT) companies, civil society organizations, investors, and academics to forge a common approach to protecting and advancing free expression and privacy online.

GNI has developed a set of Principles and Implementation Guidelines[1] to which all members commit, and which guide responsible company action when facing requests from governments around the world that could impact the freedom of expression and privacy rights of users. GNI is the only multi-stakeholder initiative with a specific focus on free expression and privacy in the ICT sector. Our vision is to create a corporate responsibility standard on freedom of expression and privacy across the industry.

Since our submission on freedom of expression in the telecommunications and internet access sector last year[2], we have taken meaningful steps to broaden our impact in promoting freedom of expression and privacy in the sector. In March 2017, GNI welcomed seven leading international telecommunications operator and vendor companies as its members. With the expanded membership, more than 1.5 billion people in over 120 countries in Africa, North, Central and South America, Europe, the Middle East and the Asia-Pacific are covered by the standards and user rights protections to which all GNI company members commit.

The theme of the Special Rapporteur's report this year, content regulation in the digital age, is one of the issues GNI gives utmost priority and attention. GNI is in a unique position to speak about the role and the impact of ICT companies in protecting freedom of speech online as several of our member companies, including Facebook, Google, Microsoft and Oath, provide

[1] GNI Principles and Guidelines are available at https://globalnetworkinitiative.org/corecommitments/index.php .

[2] GNI submission to study on Telcos and the Internet Access Sector
http://globalnetworkinitiative.org/sites/default/files/GNI-submission-SR-FOE-Telco-Report.pdf

social and search platforms to billions of customers all over the world. Recognizing that the role of companies in responding to alleged terrorist or extremist content has become one of the most challenging issues for freedom of expression and privacy online, GNI has engaged in various efforts to navigate through the challenge. 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. After a series of roundtable discussions, consultations and extensive deliberations among our participants, GNI released a policy brief on Extremist Content and the ICT Sector[3] with a detailed set of recommendations for governments and companies.

GNI is aware that many of our member companies, organizations, academics, and investors are participating in this consultation in their individual capacities through submissions, meetings, consultations, and other forms of engagement, and we hope this submission on behalf of the GNI complements those communications. We look forward to continuing to work with you as you produce this report, as well as in your broader work under this important mandate.

1. Company compliance with State laws

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 Terms of Service ("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.

According to the GNI Principles, ICT companies should comply with all applicable laws and respect internationally recognized human rights, wherever they operate. If national laws, regulations and policies do not conform to international standards, ICT companies should avoid, minimize, or otherwise address the adverse impact of government demands, laws, or regulations, and seek ways to honor the principles of internationally recognized human rights to the greatest extent possible. ICT companies should also be able to demonstrate their efforts in this regard.

The GNI Principles do not require companies to violate local law, even when that law is inconsistent with international human rights norms. However, the GNI Principles do require companies to monitor and assess risks to privacy and free expression from local laws, and to

[3] GNI, *Extremist Content and ICT Sector,* Nov 2016, available at http://globalnetworkinitiative.org/sites/default/files/Extremist-Content-and-ICT-Sector.pdf
GNI, "Extremist Content and the ICT Sector - Launching a GNI Policy Dialogue," July 1, 2015, http://globalnetworkinitiative.org/news/extremist-content-and-ict-sector-launching-gni-policy-dialogue

take measures to mitigate those risks as set forth in the GNI Implementation Guidelines. The GNI Implementation Guidelines ask participating companies to:

- Encourage governments to be specific, transparent and consistent in the demands, laws and regulations ("government restrictions and demands") that impact freedom of expression or the right to privacy, including e.g. restrictions of access to content or restrictions of communications, or demands that are issued regarding privacy in communications.

- Encourage government restrictions and demands that are consistent with international laws and standards on freedom of expression and privacy. This includes engaging proactively with governments to reach a shared understanding of how government restrictions can be applied in a manner consistent with the Principles.

- Adopt policies and procedures which set out how the company will assess and respond to government demands for restrictions to communications or access to content, or disclosure of personal information

- These policies and procedures will also address how the company will respond in instances when governments fail to provide a written directive or adhere to domestic legal procedure. They will also include a consideration of when to challenge such government restrictions and demands.

When required by governments to restrict communications, or remove content, participating companies will:

- Require that governments follow established domestic legal processes when they are seeking to (1) restrict freedom of expression or (2) access personal information.

- Request clear written communications from the government that explain the legal basis for government restrictions to freedom of expression and government demands for personal information, including the name of the requesting government entity and the name, title and signature of the authorized official.

- Keep – where the law permits verbal demands and in emergency situations, when communications will be oral rather than written – records of these demands.

- Interpret government restrictions and demands so as to minimize the negative effect on freedom of expression.

- Narrowly interpret and implement government demands that compromise privacy.

- Narrowly interpret the governmental authority's jurisdiction so as to minimize the negative effect on freedom of expression.

- Narrowly interpret the governmental authority's jurisdiction to access personal information, such as limiting compliance to users within that country.

It is recognized that the nature of jurisdiction on the internet is a highly complex question that will be subject to shifting legal definitions and interpretations over time.

When faced with a government restriction or demand that appears overbroad, unlawful, or otherwise inconsistent with domestic laws or procedures or international human rights laws and standards on freedom of expression or privacy, participating companies will in appropriate cases and circumstances:

- Seek clarification or modification from authorized officials of such requests;

- Seek the assistance, as needed, of relevant government authorities, international human rights bodies or non-governmental organizations; and

- Challenge the government in domestic courts.

Overbroad could mean, for example, where more information is restricted than would be reasonably expected based on the asserted purpose of the request.

It is recognized that it is neither practical nor desirable for companies to challenge in all cases. Rather, companies may select cases based on a range of criteria such as the potential beneficial impact on freedom of expression and privacy, the likelihood of success, the severity of the case, cost, the representativeness of the case and whether the case is part of a larger trend.

2. Responding to Other State Requests

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 TOS violation or issuing a legal order requiring content removal or restriction.

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.

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. As stated by GNI Implementation Guidelines, GNI companies are expected to refrain from entering into voluntary agreements that require the participants to limit users' freedom of expression or privacy in a manner inconsistent with the Principles. Voluntary agreements entered into prior to committing to the Principles and which meet this criterion should be revoked within three years of committing to the Principles.

3. Global removals

GNI has previously expressed its concern regarding the ruling against Google, made by Commission Nationale de L'Informatique et des Libertes (CNIL) in March 2016, requiring the global takedown of links to search information banned in France under Europe's "Right to be Forgotten". We believe that the French data protection authority's ruling sets a disturbing precedent for the cause of an open and free Internet, and sends the message to other countries that they can force the banning of search results not just inside their own jurisdictions, but assert that jurisdiction across the globe.

For this reason, we welcomed the announcement from Google that it would appeal the ruling.[4] Online search engines and intermediaries are vital tools to inform public discourse, hold the powerful to account, and highlight injustice. The right of academics, journalists, historians and all citizens to access complete and uncensored information is the bedrock of civic participation and a free society. The CNIL ruling could set the stage for a global internet where the most censored and repressive societies will effectively dictate the standard for all humanity. It is highly problematic that the authorities in one country should be able to force the global removal of search information that, even if deemed inadequate, inaccurate or irrelevant under the criteria of the Costeja ruling, is arguably still lawful, and is publicly available in other countries. That same information could also be the subject of legal protections in other countries. This includes laws that criminalize the criticism of leaders and governments, and laws that ban content pertaining to religious or ethnic minorities, LGBT people, or relating to women's health. The case will be heard the Court of Justice of the European Union after the French courts decided to refer the case in July 2017.

GNI believes this important case raises complex issues related to internationally protected rights to freedom of expression and privacy, and the ability of governments to assert jurisdiction beyond borders. We hope the Court will take the opportunity to carefully the consequences for human rights – not just in Europe, but around the world.

[4] GNI,"GNI Welcomes Appeal to the Global Reach of "The Right to be Forgotten," May 19, 2016, available at http://globalnetworkinitiative.org/news/gni-welcomes-appeal-global-reach-right-be-forgotten

4. Individuals at risk

GNI Principles are based on internationally recognized human rights laws and standards, including the Universal Declaration of Human Rights, the International Covenant on Civil and Political Right and the International Covenant on Economic, Social and Cultural Rights.
The international human rights laws and principles that form the basis for the GNI Principles include the fundamental notion that "human rights are rights inherent to all human beings, regardless of race, sex, nationality, ethnicity, language, religion, or any other status."[5]
By agreeing to abide by GNI Principles, companies are demonstrating their commitment to respect the expression of diverse views and opinions by all users without discrimination.

5. Content regulation processes

GNI member companies are required to integrate the GNI Principles into company decision making and culture through responsible policies, procedures and processes, including those related to content restrictions and takedowns, or suspension of accounts. Specifically, participating companies are asked to identify circumstances where freedom of expression and privacy may be jeopardized or advanced and integrate these Principles into their decision making in these circumstances. In our responses below on remedies and transparency, we have further articulated how these principles can be applied to content regulation practices.

6. Appeals and remedies

ICT companies should provide mechanisms for remedy that allow people who believe their account has been suspended erroneously as a result of TOS-based government referrals to seek reinstatement of their account. GNI Implementation Guidelines provide direction and guidance to companies in providing sufficient grievance mechanisms and remedies for users in order to make it possible for grievances about issues related to freedom of expression and privacy to be communicated to the company for consideration and, if appropriate, direct remediation. If a participating company determines its business practices are inconsistent with the Principles or have caused or contributed to adverse impacts, it will establish by itself or in cooperation with other actors, a means of remediation, including meaningful steps to prevent recurrence of such inconsistency or impact.

The Implementation Guidelines encourage companies to design the grievance mechanisms in accordance with the effectiveness criteria set out in principle 31 of the UN Guiding Principles on Business and Human Rights. GNI companies are also asked to provide whistleblowing

[5] "Human Rights," United Nations, accessed November 25, http://www.un.org/en/sections/issues-depth/human-rights/.

mechanisms or other secure channels through which employees can confidentially or anonymously report violations of the Principles without fear of associated punishment or retribution. For example, a company might appoint or designate an internal ombudsman, auditor or compliance officer to monitor the company's business practices which includes issues relating to freedom of expression and privacy.

7. Automation and content moderation

When used carefully and in specific, clearly defined circumstances to target specific types of content, automated tools and/or algorithmic filtering can help companies to comply with relevant law and regulations in accordance with the GNI Principles. For instance, some companies have developed and adopted algorithmic filtering tools, such as PhotoDNA,[6] for use in detecting child pornography. This tool can help companies searching for the needle of illegal content among the haystack of uploaded images. However, broad applications of automation should be carefully weighed against the risks such tools pose to freedom of expression. As GNI civil society member Center for Democracy and Technology (CDT) pointed out in a recent publication[7], companies and policy makers should recognize the limitations of such technological tools in deciphering nuance and context of text-based human communication.

If companies decide to use automation to facilitate content moderation, they should do so in a transparent, accountable manner, while maintaining an appropriate degree of human review. The process of deciding what content is addressed using automated tools, which tools are used and how, and the extent and scope of human review, should be carefully thought through in an open, transparent, participatory manner involving relevant stakeholders, so as to minimize potential human rights impacts. Governments should not mandate the use of filters or other automated content evaluation tools in laws regulating speech.

[6] https://www.microsoft.com/en-us/photodna

[7] CDT, *Mixed Messages? The Limits of Automated Social Media Content Analysis*, Nov 28, 2017, available at https://cdt.org/insight/mixed-messages-the-limits-of-automated-social-media-content-analysis/

8. Transparency

The GNI Implementation Guidelines ask member companies to operate in a transparent manner when required by government to restrict communications or access to content or provide personal information to governments. To achieve this, participating companies will:

a. Disclose to users in clear language the generally applicable laws and policies which require the participating company to remove or limit access to content or restrict communications or provide personal information to government authorities.

b. Disclose to users in a clear manner the company's policies and procedures for responding to government restrictions and demands to remove or limit access to content, restrict communications or provide personal data.

c. Give clear, prominent and timely notice to users when access to specific content has been removed or blocked by the participating company or when communications have been limited or stopped by the participating company due to government restrictions. Notice should include the reason for the action and state on whose authority the action was taken.

GNI believes that governments and ICT companies should be equally transparent about TOS-based referrals, and should seek to disclose relevant information as appropriate. 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. When governments self-identify in the course of reporting alleged violations of TOS 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. Meanwhile, 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.

9. Conclusion

The Internet has enabled an unprecedented sharing of ideas and information among billions of people around the world. Over time, the multi-stakeholder community has helped craft creative and effective responses to content-related challenges. These joint efforts have made the Internet safer and more accessible, while preserving the space for critical and challenging engagement, as well as the open and interoperable architecture that has allowed it to thrive. GNI and its members are committed to continuing to engage in multi-stakeholder dialogue to ensure that the open, interoperable internet continues to expand and facilitate free expression globally. We thank the Special Rapporteur for his attention to this very important matter and look forward to future collaboration in advancing human rights in the Digital Age.