

29 January 2016

UN Special Rapporteur David Kaye
Office of the United Nations High Commissioner for Human Rights
Geneva, Switzerland



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

RE: Submission to study on private ICT sector responsibilities

The Global Network Initiative (GNI) welcomes the opportunity to provide input for the report that the Special Rapporteur on the protection and promotion of the right to freedom of opinion and expression, David Kaye, is preparing on the responsibilities of the Information and Communication Technology (ICT) sector to protect and promote freedom of expression in the digital age.

The GNI brings together ICT companies with civil society organizations, investors, and academics to forge a common approach to protecting and advancing free expression and privacy online. The GNI has developed a set of Principles and Implementation Guidelines to guide responsible company, government, and civil society action when facing requests from governments around the world that could impact the freedom of expression and privacy rights of users.

I. Aspects of GNI companies' operations that implicate the right to freedom of expression

The GNI Principles address the challenges that arise for a broad range of ICT companies when demands from government authorities impact the freedom of expression and privacy rights of their users. In 2011, the GNI commissioned the report *Protecting Human Rights in the Digital Age*, which outlines areas of risk for different parts of the sector.¹

The transparency reports published by many ICT companies highlight the types of government demands that are received and inform users how these demands are addressed. In terms of our current company membership, the most frequent types of demands that implicate the right to freedom of expression are those that aim to remove user-generated content from online platforms and to block the results that a search engine returns when a particular term is entered. In several states, online services are also compelled to block or filter content that is deemed unlawful or they may face liability as a host. Furthermore, government demands to suspend user accounts or to identify anonymous users impact the right to freedom of expression.²

¹ Dunstan Allison Hope, *Protecting Human Rights in the Digital Age*, BSR and the Global Network Initiative (2011), available at: http://globalnetworkinitiative.org/sites/default/files/files/BSR_ICT_Human_Rights_Report.pdf

² For more information on the ways in which the operations of online intermediaries impact freedom of expression, see Rebecca MacKinnon et al., *Fostering Freedom Online: The Role of Internet Intermediaries*, UNESCO (2014).



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

ICT companies may also affect freedom of expression when setting content policies under terms of service, which reflect their brand and nature of their services.³ Policies will vary depending on the different nature and type of services provided.

II. Key legal and policy issues in the ICT sector that implicate freedom of opinion and expression

Companies participating in the GNI face the greatest challenge in implementing the GNI Principles when governments seek to restrict the rights to freedom of expression and privacy in a way that is inconsistent with the principles of legality, necessity, and proportionality. We have highlighted five key legal and policy issues in which this challenge is particularly acute.

A. Laws on intermediary liability

Around the world, calls for service providers to police user content and communications, under threat of greater liability, and at times under broad and vague standards of what content is considered illegal, continue to be highly problematic for freedom of expression. Carriers and conduits enable worldwide scale and availability of information by automatically transmitting or storing words, pictures, and videos created by individuals. Policies creating liability for carriers on the basis of content sent or created by users threaten to chill freedom of expression by incentivizing carriers to restrict the use of their services for any content that could be considered controversial, or to restrict the pseudonymous use of these services. This impetus is particularly strong where definitions of illegal content are vague and overbroad, incentivizing self-censorship and prior restraints on speech.⁴

Similarly, the GNI is deeply troubled by the risks to freedom of expression and access to information presented by court decisions and proposed laws that allow individuals to compel search engines to remove links to unwanted information, even if that information is accurate, lawful, and publicly available elsewhere (often termed “the right to be forgotten”). This policy is particularly problematic when the burden is placed on companies, rather than courts, to make the ambiguous distinction between the right to privacy and the right to seek and impart information. When companies decide that the scales tip in favor of free expression, they may still face legal action from data protection offices and other court orders to alter or remove access to otherwise publicly accessible information.

³ The GNI conducted a learning series on this subject which led to publication of the following report: Erica Newland et al., *Account Deactivation and Content Removal: Guiding Principles and Practices for Companies and Users*, the Berkman Center for Internet & Technology and the Center for Democracy and Technology (2011), available at: https://cdt.org/files/pdfs/Report_on_Account_Deactivation_and_Content_Removal.pdf

⁴ See Manila Principles on Intermediary Liability, available at: www.manilaprinciples.org.



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

B. Broad laws prohibiting extremist content and promotion of terrorism

A related issue is the acceleration of government demands on ICT companies to remove alleged terrorist or extremist online content. The GNI acknowledges the legitimate national security and law enforcement obligations of governments. At the same time, there continues to be no internationally agreed upon definition of terrorism. National laws 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. Definitions of content that is “extremist” are often broad, and across the world, counterterrorism laws have been used to imprison journalists, bloggers, lawyers, and human rights defenders.

As part of their efforts to prevent online radicalization, some authorities have suggested that ICT companies should face criminal liability for failing to delete content praising terrorism from their platforms.⁵ Others have attempted 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 and accountability 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 them to review against their own content policies, and Europol has extended this approach via the creation of an Internet Referral Unit that would coordinate referrals across the EU.

C. Proposals to weaken encryption standards

As your 2015 report to the Human Rights Council recognizes, encryption and anonymization technologies are enablers of the right to freedom of expression. Encrypted communications are particularly important for journalists, lawyers, and human rights defenders—people who need to be able to communicate confidentially with sources—by mitigating the threat of surveillance.

The GNI continues to be concerned by government proposals and practices that would compromise the digital security of individuals to pursue law enforcement objectives. Of particular concern are government mandates that companies provide back doors into hardware or software or demands that companies take steps that would compromise the security of user's communications. The GNI advocates for governments to support strong encryption and not to subvert security standards.⁶

⁵ See, e.g., European Parliament resolution of 25 November 2015 on the prevention of radicalisation and recruitment of European citizens by terrorist organisations (2015/2063(INI)).

⁶ Global Network Initiative, Submission to UN Special Rapporteur on the Protection and Promotion of the Right to Freedom of Expression and Opinion (February 2015), available at: <http://www.globalnetworkinitiative.org/sites/default/files/GNI%20Submission%20on%20Encryption.pdf>



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

D. The need for Mutual Legal Assistance reform

The Mutual Legal Assistance (MLA) regime is the dominant and widely accepted method for managing lawful government-to-government requests for data across jurisdictions. However, the regime has not been updated to keep pace with globalized data, making the process inefficient and opaque, and requests to the U.S. government take an average of 10 months to fulfill.⁷ As a result, authorities from other governments sometimes resort to drastic measures. Some states have attempted to demand that their domestic laws apply extraterritorially, have proposed data localization measures, and have sought to compromise the digital security of individuals. These measures would be harmful to an open, robust, and free Internet, and reforms to the current MLA regime are urgently needed in order to prevent the evolution of policy in this direction.

The GNI has identified a series of practical and legal reforms that policymakers could adopt in order to reform the current MLA system.⁸ We also support efforts to develop a new international legal framework to enable foreign law enforcement authorities to receive efficient access to information in pursuit of legitimate law enforcement objectives when access is consistent with international norms on human rights and privacy. GNI supports reforms to cross-border law enforcement data requests which would allow governments to make requests for data from providers, as long as stringent human rights requirements apply and the process is characterized by robust transparency, accountability, and international credibility.

E. The need for greater government transparency

The GNI has advocated for greater transparency when governments debate laws, regulations, and policies that impact the freedom of expression and privacy of Internet users globally. The GNI urges both governments and intergovernmental organizations to take a transparent approach, ensuring that any measures that affect these rights are subject to public debate and consulted with a broad group of stakeholders and experts. A number of ICT companies have taken steps to be more transparent with their users about the requests they receive from governments, including by publishing transparency reports. Governments participating in the Freedom Online Coalition have also started to signal a willingness to make improvements on transparency. Nevertheless, it is essential that all governments take steps to be more transparent about the laws and legal interpretations that authorize electronic surveillance or content removal. Governments should also issue reports on the aggregate numbers of requests that they make to ICT companies and the number of users impacted by these requests, and they should permit companies to issue analogous reports.⁹

⁷ See, e.g., *Liberty and Security in a Changing World*, Report and Recommendations of the President's Review Group on Intelligence and Communication Technologies, 227 (12 December 2013).

⁸ Andrew K. Woods, *Data Beyond Borders: Mutual Legal Assistance in the Internet Age*, Global Network Initiative (January 2015), available at: <https://globalnetworkinitiative.org/sites/default/files/GNI%20MLAT%20Report.pdf>

⁹ Susan Morgan and Emma Llansó, *Getting Specific about Transparency, Privacy, and Free Expression Online*, Global Network Initiative (5 November 2014), available at:



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

III. The Global Network Initiative and its Principles

Launched in 2008, the GNI is a multistakeholder initiative that brings together over 40 organizations to forge a common approach to free expression and privacy online.¹⁰ The GNI Principles are based on internationally recognized laws and standards for human rights set out in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the International Covenant on Economic, Social and Cultural Rights. The “Protect, Respect and Remedy” Framework, ultimately codified as the UN Guiding Principles, also informed the development of the GNI Principles.¹¹

International organizations, experts, and government officials have cited membership in the GNI and adherence to its Principles as good practice for ICT companies that seek to fulfill their responsibilities under the UN Guiding Principles on Business and Human Rights.¹² The GNI Principles, Implementation Guidelines and tools can inform responsible decision-making when companies face requests from governments around the world that could impact the freedom of expression and privacy rights of users; they may also be used to assess human rights risk when entering or leaving a market or when designing and introducing new technologies, products or services. Moreover, the GNI accountability process uses independent assessment to verify that companies are implementing the principles. By working together with human rights groups, press freedom organizations, investors and academics, ICT companies can manage human rights challenges, maintain credibility and support the privacy and freedom of expression rights of their users.

In 2013, the GNI conducted its first assessment of the compliance of its three founding companies – Google, Microsoft, and Yahoo – with the GNI Principles.¹³ In November of 2014, the Board reviewed self-reporting from newer company members, including Facebook and LinkedIn.¹⁴ In 2015, independent assessments will be conducted of all five participating companies.

<http://globalnetworkinitiative.org/news/getting-specific-about-transparency-privacy-and-free-expression-online>

¹⁰ For a list of GNI participants, see <http://globalnetworkinitiative.org/participants/index.php>

¹¹ See <http://globalnetworkinitiative.org/corecommitments/index.php>

¹² See, e.g., *The Role of Internet Intermediaries in Advancing Public Policy Objectives*, DSTI/ICCP(2010)11/FINAL, Organisation for Economic Co-operation and Development, 33-35 (22 June 2011); Hillary Rodham Clinton, United States Secretary of State, Remarks on Internet Freedom, Washington, D.C. (January 21, 2010); Uri Rosenthal, Minister of Foreign Affairs of the Netherlands, Speech on respecting freedom of expression online, Brussels (24 March 2011); Shift and Institute for Human Rights and Business, *European Commission ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights*, 18-19, 34, 43, 45, 61 (2013); *The Right to Privacy in the Digital Age*, Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/27/37, paras. 44-46 (30 June 2014); *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Frank La Rue, A/HRC/17/27, para. 46 (16 May 2011).

¹³ Global Network Initiative, *Public Report on the Independent Assessment Process for Google, Microsoft, and Yahoo* (January 2014), available at: <http://globalnetworkinitiative.org/sites/default/files/GNI%20Assessments%20Public%20Report.pdf>

¹⁴ Global Network Initiative, *2014 Annual Report*, available at: <https://globalnetworkinitiative.org/sites/default/files/2014%20Annual%20Report.pdf>



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

Finally, a key element of membership in the GNI for all stakeholders is the opportunity for shared learning. Learning occurs through periodic conference calls exploring specific situations that implicate the GNI Principles, through public learning forums and participation in international conferences,¹⁵ and through smaller roundtable discussions that explore policy issues.¹⁶ These learning activities not only contribute to responsible company decision-making, but they also inform the research, advocacy, and policy activities of a broad range of individuals and organizations.

Thank you for the opportunity to contribute to this report. We would be pleased to engage further on this subject if desired.

Sincerely,

Judith Lichtenberg
Executive Director

¹⁵ See, e.g., Global Network Initiative, *GNI and Stanford Host Privacy, Security, and Freedom of Expression Learning Day at Stanford University on December 2nd*, December 2, 2015.

¹⁶ See, e.g., Global Network Initiative, *GNI and CDT host closed roundtable session in London on regulating of extremist content online*, October 30, 2015.