

Global Network Initiative

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

Written Statement for Senate Judiciary Subcommittee on Human Rights and the Law “Global Internet Freedom and the Rule of Law, Part II”

March 2nd, 2010

The Global Network Initiative (GNI) welcomes the opportunity to discuss internet freedom and the rule of law with the Senate Judiciary Subcommittee on Human Rights and the Law.

All over the world - from the Americas to Europe to the Middle East to Africa and Asia - companies in the ICT industry face increasing government pressure to comply with domestic laws and policies that require censorship and disclosure of personal information that conflict with internationally recognized human rights laws and standards.

In an effort to protect and advance the human rights of freedom of expression and privacy, a diverse coalition of leading information and communications technology (ICT) companies, major human rights organizations, academics and investors launched the GNI in October 2008.

The GNI is founded upon Principles on Freedom of Expression and Privacy and supported by specific implementation commitments and a framework for accountability and learning. Together, this framework provides a systematic approach for companies, NGOs, investors, academics and others to work together in resisting efforts by governments that enlist companies in acts of censorship and surveillance that violate international standards.

The Initiative is founded on the internationally recognized laws and standards for human rights on freedom of expression and privacy set out 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”).

These three features – foundation upon international human rights standards, a multi-stakeholder approach and global applicability – underpin the unique value of the GNI. It is our belief that the organization has the potential to lead the way in helping companies make decisions that protect the freedom of expression and privacy rights of hundreds of millions of Internet users around the world. However, there are two inter-related issues that must be addressed if the GNI is to reach its full potential and maximize its positive impact on human rights:

1. While the GNI’s top-level Principles are relevant across the whole ICT ecosystem – equipment manufacturers, software providers, search engines, consumer electronics companies and telecommunications services providers – there are business and human rights issues impacting this sector (such as sales of filtering software or surveillance equipment) that the GNI’s Implementation Guidelines may not address. We need broad stakeholder input to fashion guidelines to incorporate these issues.
2. Even among Internet services companies for whom the existing Principles and Implementation Guidelines are on point, participation has not expanded beyond the original three US internet companies. Respect for internationally recognized rights of freedom of expression and privacy will most likely advance where a broad cross-section of companies makes this commitment, and so it is important that a much larger number of companies participate in the GNI’s work.

1. GNI Implementation Dialogue – Drawing from the Whole ICT Ecosystem

The GNI Principles and Implementation Guidelines were drafted using a multi-stakeholder approach involving companies, investors, academics and NGOs. Among the companies were global internet and telecommunications firms and for this reason the content of the GNI's Principles and Implementation Guidelines reflects the specific circumstances faced by these companies.

While the top-level GNI Principles are relevant to firms across the ICT sector, we recognize that GNI's Implementation Guidelines require some adaptation or supplementation in order to more directly guide companies in other segments of the ICT industry, such as equipment manufacturers, consumer electronics brands, handset manufacturers and the providers of security and filtering services, enterprise management software and databases. The GNI has established an "Implementation Dialogue" to achieve this objective.

Since the launch of the GNI in October 2008 the organization has engaged in conversations with a wide variety of ICT companies including semiconductor manufacturers, software providers, equipment manufacturers, consumer electronics brands and telecommunications services providers. These conversations have tended to converge on three important questions:

- What do ICT companies view as their main privacy and freedom of expression risks and opportunities?
- What do these risks and opportunities reveal about the relevance of the existing GNI Principles and Implementation Guidelines?
- Can the existing GNI Implementation Guidelines be adapted or supplemented to increase their relevance to a wider range of ICT companies?

Despite the diversity of companies that together constitute the whole ICT industry, views about the relevance of the existing GNI Principles and Implementation Guidelines have been remarkably consistent.

First, and very importantly, there are large sections of the GNI documents that are entirely relevant to the whole ICT industry. This includes, for example, the top level Principles, and the commitments relating to responsible company decision making, human rights impact assessments and multi-stakeholder collaboration to advance human rights.

Second, there are four areas where GNI can take the lead in developing standards to increase the relevance of the Implementation Guidelines to a wider range of ICT companies. Here we set out these four interrelated questions in more detail and they will guide the GNI Implementation Dialogue to bring more companies into GNI.

i. Understanding freedom of expression and privacy risk associated with product functionality.

The GNI's Implementation Guidelines are currently focused on the level of the *content* (e.g. circumstances in which a company should/ should not remove content) and at the level of *personal information* (e.g. circumstances in which a company should/ should not disclose personal information to law enforcement agencies).

However, to become relevant for a wider group of companies, we need to explore how the GNI documents may apply at the level of the *product functionality* – in other words, what impact the product functionality created by the ICT company can have on freedom of expression and privacy. One example would be how firms should respond if governments were to mandate the

installation of censorship capabilities in products, such as devices or software. Key questions include:

- What ability does an ICT company have to design or control the functionality of products to minimize censorship or illegitimate access to personal information? For example, this could include network equipment functionality that enables intercept and surveillance, or pre-installed products in consumer electronics such as filtering and surveillance software.
- Are there ways to design future ICT networks or create global product standards that will minimize risks to privacy and freedom of expression at every stage of the ICT value chain?
- How can ICT companies collaborate on a common freedom of expression and privacy agenda given that multiple companies' products work together as parts of one overall, interdependent network?

ii. Human rights due diligence on who ICT companies sell to, and understanding the intended use of the ICT product, service, technology or functionality.

The GNI Implementation Guidelines already have content relating to the use of human rights risk assessments to inform company strategies and approaches to freedom of expression and privacy. However, to be more relevant and useful for a wider group of ICT companies, the following questions would need to be explored in further depth:

- How can ICT companies assess the risk that customers (e.g. public sector) will use the product, service, functionality or technology being provided to violate human rights?
- What strategies can be put in place to mitigate that risk?
- What would due diligence look like at the level of the country (i.e. market entry or exit) and at the level of the customer (i.e. customers a company could choose not to sell to)?
- There are many relevant laws that already exist for customer relationships in high risk locations (e.g. export control laws), but what guidance or criteria may exist beyond this for customer engagements that may be 'legal but unethical', or which may be invasive of privacy and freedom of expression?
- How can an ICT company interpret the intended use of the ICT product, service or technology when the same functionality can be used for good or for ill? For example, the same functionality that allows remote access to a PC for maintenance and trouble shooting can have more negative applications too. What are the boundaries of responsibility for the ICT company?

iii. Many ICT companies provide consulting advice alongside the product, service or technology.

Many ICT companies not only provide hardware or software products "off the shelf" but also provide consulting advice and guidance on how to make the best use of the product or service. While it certainly can be difficult to "understand the intent" when selling a product or service "off the shelf", this position is less credible when consulting services are provided to customers alongside the product. Some questions to explore include:

- What kinds of consulting services are provided that might advise customers on how to use products for censorship or to facilitate illegitimate access to personal information?

- Can human rights guidelines be provided on the types of consulting advice that should be provided?
- What responsibility does the ICT company have if the advice about the use of their products is provided by contractors that are independent of the company – but who may have been trained by them?

iv. Responding to government demands and mandated standards.

There is a concern that companies are going to increasingly receive requests and demands from governments to modify hardware and software products in ways that will make them more freedom of expression or privacy invasive – for example, by mandating certain product functionalities or software installations. There is a great deal of content in the GNI Implementation Guidelines on how to respond to government demands, but (as described above) these cover the level of the *content or personal information*, not the level of the *functionality*. Questions include:

- How should ICT companies' respond to government demands to alter functionality or adhere to certain product standards?
- How can ICT companies collaborate with each other and with other stakeholders in response to such mandates?

2. Increasing Company Participation in the GNI

The GNI has been seeking to substantially increase company participation in its activities. These recruitment efforts started long before the GNI was launched and have continued till this day – but so far without success at securing new membership commitments. Questions from prospective member companies about GNI and its value for business are important and worth asking; participation in GNI is a meaningful commitment that we do not anticipate companies should undertake lightly. At the same time, we believe that GNI has been conscious of these legitimate concerns and responsive to them. Here we describe the five main reasons that we frequently hear from companies for not participating in the GNI, and summarize our response to those concerns.

i. “GNI’s Principles and Implementation Guidelines are not relevant to our company’s business”

- The core commitments in GNI are relevant to the entire ICT industry.
 - Protect and advance freedom of expression
 - Support responsible company decision making
 - Conduct human rights impact assessments
 - Collaborate with multiple stakeholders to advance human rights
- Companies that transmit information, sell network equipment, publish content, sell filtering software, or hold user data – including wired and wireless telecommunications carriers, web hosting companies, online service providers, content producers, entertainment and news media outlets, hardware and device manufacturers, and software designers – can have direct and indirect impacts on freedom of expression and privacy.
- By offering tools and a framework to support human rights due diligence and risk assessments, GNI can help all ICT companies make more responsible decisions about new products and services, potential partnerships, and market entry.

- Global telecommunications companies participated in drafting GNI's Principles and Implementation Guidelines, reflecting the interests of a broader range of companies.
- Freedom of expression and privacy are important to the entire Internet ecosystem – given the role of the private sector in building and operating this ecosystem, working together to improve respect for these rights should be part of every company's consideration of the social impacts of its operations. GNI is not only a remedial exercise for companies who have had learning experiences or challenges – it is a systematic way to improve the policy environment and help protect the well-being of individual users and customers in the ICT sector.

ii. “No other companies like ours have joined, and we don’t want to make our company stand-out by joining alone”

- GNI is an opportunity to show pro-active leadership, foresight, and responsible corporate practices – something which generally is an attractive way to stand out. The ICT sector has been for some time in an era of tension between the entrepreneurial energy that leads to innovation on the one hand and society's interests in regulating technologies that are now a fundamental element of modern society on the other - tension exacerbated by the fact that social norms and their associated legal frameworks change more slowly than technologies. Every company in the ICT sector has a stake in helping to see that their own practices and their engagement in public policy navigate this era with credible guidance and with attention to preserving principles such as free expression and privacy.
- GNI provides a systematic way for companies to learn together with relevant stakeholders and socialize data about the challenges they face. Companies who are concerned about ‘standing out’ in terms of attracting unwanted attention should understand GNI does not have this intent.

iii. “The assessment process is too burdensome, raises legal concerns such as confidentiality, or is not suited to our company’s products and services”

- The independent assessment process is critical to credibility – only through independent assessment can GNI effectively demonstrate that companies are following through on the commitments they have made and that GNI is meeting its commitment to operate in a principled, pragmatic and constructive way.
- The assessment process is primarily about learning. During the assessment process, we will learn what is working and what is not with the GNI Principles and Implementation Guidelines and make changes to our approach accordingly.
- A wide range of legal concerns (such as confidentiality requirements, trade secrets, attorney-client privilege, legal constraints) have been raised and addressed in the design of the assessment process to make it workable for companies. Google, Yahoo! and Microsoft would not be participating if the assessments had not addressed these concerns.
- Companies will be active participants in the assessment process; for example, they will select their own assessors, drawing from a pool of assessors accredited by the GNI.

iv. “GNI commitments are too burdensome for small companies to implement”

- While membership requires executive-level commitment to the principles and GNI framework, implementation of GNI commitments will vary for each company, depending on differences in size, markets, business models, products, and services.

- Assessment of a company's compliance will take the individual company's resources and business context into account. There is no "one-size fits all" approach to implementation and GNI fully anticipates that companies will find ways to implement its commitments in ways appropriate to the size, scale and scope of the participating company.

v. "Our company can implement the GNI Principles ourselves without joining GNI"

- GNI's Principles and Implementation Guidelines are in the public domain; companies can always follow the guidance GNI offers. However, a companies-only effort doesn't offer the public credibility or effectiveness of the multi-stakeholder approach. GNI is the only effort today in the ICT sector that is multi-stakeholder and that offers a third-party assessment process.
- GNI has been developed through nearly four years of intensive negotiation, collaboration, and public scrutiny and includes the commitment of some of the most prominent NGOs (Human Rights Watch, Center for Democracy & Technology, Human Rights First, Electronic Frontier Foundation, Human Rights in China, Committee to Protect Journalists, and others), academics (from Harvard, Berkeley, USC, St. Gallen, and others), and socially responsible investors (Calvert, Boston Common, F&C, Domini, and others).
- GNI enables stakeholders to come together and address global challenges and common responsibilities, and collectively create, implement, and evaluate mechanisms to protect and advance freedom of expression and privacy. An important part of how industry and civil society address these issues will be the extent to which there is a shared commitment across a broad set of stakeholders. Implementation of the principles and guidelines is important, but a shared public commitment to advance rights to freedom of expression and privacy is also an important objective, which individual implementations cannot address as effectively.

3. A shared, public, credible commitment by all companies is essential to protecting the rights to freedom of expression and privacy

It is essential that the global ICT industry and its stakeholders make a public and shared commitment to respect user rights in the face of increased threats to freedom of expression and privacy. The ICT industry is diverse, and different companies may make different decisions about entering or exiting a market based on specific circumstances such as timing, location, relationships and the nature of a particular product, service or business. There is no "one size fits all" approach to corporate responsibility, nor a single right course of action or script for all to follow. We invite all ICT companies to participate in the GNI and draw upon the guidance and insights provided by the GNI's principles and guidelines in creating a responsible approach to business decisions.

The GNI also meets Secretary of State Clinton's call for ICT companies to be able to operate in a manner that promotes respect for human rights, even in the most challenging markets. The GNI provides principles, guidelines and support to ICT companies, helping them to think through difficult choices and make decisions that protect freedom of expression and privacy for hundreds of millions of Internet users around the world.

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 participating in the GNI and working together with human rights groups, investors and academics, ICT companies can benefit from valuable collaboration, accountability, confidential input and collective action. These resources can help companies manage these challenges, maintain credibility and support the privacy and freedom of expression rights of their users.

The GNI's guidelines indicate that companies should:

- Establish human rights risk assessment procedures and integrate the findings into business decision-making
- Require that governments follow established domestic legal processes when they are seeking to restrict freedom of expression and privacy
- Provide users with clear, prominent and timely notice when access to specific content has been removed or blocked
- Encourage governments, international organizations and entities to call attention to the worst cases of infringement on the human rights of freedom of expression and privacy
- Utilize independent assessments of company implementation of the GNI's principles

4. Conclusion

Thank you for the opportunity to comment. GNI is committed to working with the Committee, companies, and other stakeholders to advance the respect and protection for freedom of expression and privacy around the world.