

December 8, 2011

UN Working Group on Human Rights and Transnational Corporations  
and Other Business Enterprises

Mr. Michael Addo (Ghana)  
Ms. Alexandra Guaqueta (Colombia / USA)  
Ms. Margaret Jungk (USA)  
Mr. Puvan Selvanathan (Malaysia)  
Mr. Pavel Sulyandziga (Russian Federation)



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

Dear Mr. Addo, Ms. Guaqueta, Ms. Jungk, Mr. Selvanathan, and Mr. Sulyandziga:

The Global Network Initiative (GNI) welcomes the opportunity to engage with the UN Working Group on Human Rights and Transnational Corporations and Other Business Enterprises as it determines its key thematic priorities and opportunities. We propose that the issues of free expression and privacy in the information and communications technology (ICT) sector be a focus for the working group. The office of UN Special Representative for Business and Human Rights John Ruggie served as an observer of GNI during its mandate, and we look forward to building on our prior exchanges with the office of the Special Representative as we serve as a resource to you.

With billions of people around the world using Information Communication Technology (ICT), the decisions that companies make in this sector—about where they store their data and how they respond to government requests, to name just a few—can have far-reaching human rights consequences. These are not easy issues. Governments have a responsibility to preserve national security, however they do not always do so in ways consistent with other fundamental rights including freedom of expression and privacy. Recent events from the Arab Spring to the initial reaction of the UK government to the riots in London have demonstrated the importance of these issues to companies in many countries they operate in around the world. More companies than ever, operating across the ICT sector, face significant scrutiny regarding their human rights policies and practices.

GNI is founded upon Principles of 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 and academics to work together in resisting efforts by governments that enlist companies in acts of censorship and surveillance that violate international standards. Attached is a copy of our 2010 Annual Report, as well as a BSR report commissioned by GNI that examines the freedom of expression and privacy risks across the ICT sector.

Through GNI's Principles, GNI's participants seek to implement a standard for freedom of expression and privacy in the ICT sector that is consistent with the UN's Protect, Respect, and Remedy framework. The first round of independent assessments of company implementation of our Principles are currently underway. GNI has also served as a platform for collective action on policy, speaking out on issues ranging from the shutdown of the Internet in Egypt, to social media and unrest in London, to the free expression implications of intellectual property enforcement legislation proposed in the United States.

GNI welcomes the important steps forward taken by UN and other intergovernmental organizations during the past year on the business and human rights agenda as it relates to the ICT sector. These include the endorsement by the UN Human Rights Council of the Guiding Principles for Business and Human Rights and the establishment of your working group, as well as the references to human rights and Internet freedom in the in the OECD's recent update of the

Guidelines for Multinational Enterprises, and the consideration of key issues around intermediary liability and the protection of privacy in the report of Frank La Rue, UN Special Rapporteur on Freedom of Opinion and Expression.

The increasing importance and ubiquity of ICTs in daily life has increased the impact of technology policy upon fundamental human rights, and placed the ICT sector at the center of global dialogue around business and human rights. GNI commends you on your appointment to the Working Group, looks forward to engaging with you as you fulfill your mandate, and recommends that you make freedom of expression and privacy in the ICT sector a priority. We welcome the opportunity to serve as a unique multi-stakeholder resource for your work, and we would welcome the opportunity to meet with you.

Sincerely,

A handwritten signature in black ink, appearing to read "Susan Morgan", with a stylized flourish at the end.

Susan Morgan  
Executive Director of the Global Network Initiative

*GNI is a multi-stakeholder group of companies, civil society organizations (including human rights and press freedom groups), investors and academics, who have created a collaborative approach to protect and advance freedom of expression and privacy in the information and communication technologies (ICT) sector. GNI provides resources for ICT companies to help them address difficult issues related to freedom of expression and privacy that they may face anywhere in the world. GNI has created a framework of principles and a confidential, collaborative approach to working through challenges of corporate responsibility in the ICT sector.*



# Protecting Human Rights in the Digital Age

Understanding Evolving Freedom of Expression and Privacy Risks in the Information and Communications Technology Industry

Dunstan Allison Hope, BSR  
February 2011



## About This Report

This report was commissioned and funded by the Global Network Initiative (GNI) and written by Dunstan Allison Hope at BSR. The report is based on literature review as well as interviews with individuals in the Information and Communications Technology industry. The author would like to thank the interviewees for their perspectives. Any errors are those of the author. Please direct comments or questions to Dunstan Allison Hope at [dhope@bsr.org](mailto:dhope@bsr.org).

Dunstan Allison Hope is a Managing Director at BSR and co-author (with Andy Wales and Matthew Gorman) of *Big Business, Big Responsibilities* (Palgrave Macmillan, 2010).

### **DISCLAIMER**

BSR publishes occasional papers as a contribution to the understanding of the role of business in society and the trends related to corporate social responsibility and responsible business practices. BSR maintains a policy of not acting as a representative of its membership, nor does it endorse specific policies or standards. The views expressed in this publication are those of its author and do not necessarily reflect those of BSR members or the Global Network Initiative.

### **ABOUT BSR**

A leader in corporate responsibility since 1992, BSR works with its global network of more than 250 member companies to develop sustainable business strategies and solutions through consulting, research, and cross-sector collaboration. With offices in Asia, Europe, and North America, BSR uses its expertise in the environment, human rights, economic development, and governance and accountability to guide global companies toward creating a just and sustainable world. Visit [www.bsr.org](http://www.bsr.org) for more information.

### **ABOUT THE GLOBAL NETWORK INITIATIVE**

The Global Network Initiative (GNI) is a multi-stakeholder group of companies, civil society organizations (including human rights and press freedom groups), investors and academics dedicated to protecting and advancing freedom of expression and privacy in the Information and Communications Technology (ICT) sector. To learn more, visit [www.globalnetworkinitiative.org](http://www.globalnetworkinitiative.org).

# Contents

## **1 Introduction**

Importance of Thinking Systemwide

Human Rights Context

Law Enforcement and National Security Context

National and Local Context

Importance of Dialogue

## **2 Executive Summary**

## **3 Characteristics of ICT and Human Rights**

## **4 ICT Industry Map**

## **5 Freedom of Expression and Privacy Risk Drivers in the ICT Industry**

Telecommunications Services

Cell Phones and Mobile Devices

Internet Services

Enterprise Software, Data Storage, and IT Services

Semiconductors and Chips

Network Equipment

Consumer Electronics

Security Software

## **6 Conclusions**

Relationships with Governments

Designing Future Networks

Implementing Due Diligence

Engaging Employees, Users, and Consultants

## 1. Introduction

We live in a world today where vast Information and Communications Technology (ICT) infrastructures and extensive flows of information have become natural and unquestioned features of modern life. Rapidly growing online services—everything from social media to ecommerce and virtual collaboration—have come to define our day-to-day lives in ways unimaginable just a decade ago.

Yet the role of ICT in society continues to evolve at a rapid pace, with new developments constantly altering the interaction between ICT and the way we lead our lives. Whether it is the increasing use of mobile devices to access internet content, the trend toward remote storage (“cloud computing”), or the rapid growth of user-generated content and social networking, the characteristics of the ICT industry and its interaction with society are in constant flux. Seemingly innocuous changes to the ICT landscape—such as altering the internet domain name system to allow non-roman characters, or massively increasing the number of IP addresses—can have significant social implications. A world in which a car is also a computer and household devices are connected to the internet (the so-called “internet of things”) will be a very different place.

This increasingly pervasive, unpredictable, and rapidly changing interaction between ICT and society brings with it a wide range of new human rights risks and ethical dilemmas for companies in the ICT industry, especially for how to protect and advance freedom of expression and privacy online. The way in which private sector corporations respond to these risks and dilemmas will affect the lives of billions of ICT users all around the world.

---

This increasingly pervasive, unpredictable, and rapidly changing interaction between ICT and society brings with it a wide range of new human rights risk drivers and ethical dilemmas for companies in the ICT industry, especially for how to protect and advance freedom of expression and privacy online.

---

### Importance of Thinking Systemwide

In many countries internet companies have faced demands to restrict access to websites, remove user-generated content, or provide personal information to law enforcement agencies. Risks to the human rights of freedom of expression and privacy are relevant to the entire ICT value chain, however. The debate about the use of ICT infrastructure for surveillance during the Iranian elections raised questions for the providers of telecommunications network equipment. The closure of entire mobile telecommunications networks in Egypt exposed the vulnerability of telecommunications services providers to government demands. The “Green Dam Youth Escort” proposals in China<sup>1</sup> were of great concern to computer makers. And demands from the governments of UAE, Saudi Arabia, and India (among others) to access messages sent over BlackBerry devices piqued the interest of handset makers everywhere.

---

<sup>1</sup> Announced in spring 2009, these proposals (subsequently defeated) would have mandated the pre-installation of filtering software on all computers sold in China, including those manufactured abroad.

---

This assertion—that states have a duty to protect human rights and companies have a responsibility to respect them—is consistent with the framework set out by the Special Representative of the United Nations Secretary-General for Business and Human Rights. The UN Human Rights Council unanimously welcomed this framework in June 2008.

---

---

A key premise of this report is our expectation that the ICT industry will be affected by two separate yet related trends taking place simultaneously: The scale of human rights expectations of business is on the rise just as developments in technology make human rights risks and opportunities far more significant for the industry.

---

All these events have projected the spotlight on a range of human rights issues that exist throughout the ICT value chain. Network equipment, consumer electronics devices, telecommunications services, enterprise and security software, IT services, and mobile devices together form an entire ICT ecosystem and all have their parts to play. Designing and operating ICT networks that effectively protect and respect human rights requires an understanding of human rights risk at each stage of the ICT value chain, and how each part interacts.

## Human Rights Context

This report provides a description of the overall ICT ecosystem and maps freedom of expression and privacy risk drivers against each description.

When referring to the human rights of privacy and freedom of expression, this report takes as its starting point the 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.

All human rights are indivisible, interdependent, and interrelated: the improvement of one right facilitates advancement of the others; the deprivation of one right adversely affects others. Freedom of expression and privacy are explicit parts of this international framework of human rights and are enabling rights that facilitate the meaningful realization of other human rights.

The duty of governments to respect, protect, promote, and fulfill human rights is the foundation of this human rights framework. That duty includes ensuring that national laws, regulations, and policies are consistent with international human rights laws and standards on freedom of expression and privacy. At the same time, ICT companies have the responsibility to respect the freedom of expression and privacy rights of their users.

This assertion—that states have a duty to protect human rights and companies have a responsibility to respect them—is consistent with the framework set out by the Special Representative of the United Nations Secretary-General for Business and Human Rights. The UN Human Rights Council unanimously welcomed this framework in June 2008. In November 2010 the Special Representative provided recommendations for how this framework can be put into practice by companies, such as undertaking human rights risk assessments, developing structures and processes for the management of human rights, and publicly communicating human rights impacts.

BSR anticipates that governments, civil society, and consumers will, over the coming years, increasingly expect large companies to be proactive in the identification of human rights risks and opportunities, and be deliberate in their management. Indeed, a key premise of this report is our expectation that the ICT industry will be affected by two separate yet related trends taking place simultaneously: The scale of human rights expectations of business is on the rise just as developments in technology make human rights risks and opportunities far more significant for the industry.

## Law Enforcement and National Security Context

The relationship between human rights, companies, governments, law enforcement agencies, and national security concerns are especially prominent in this report, and in this regard it is very important to be clear about two particular features of these relationships:

---

The contrast between these two features of the relationships among national security, law enforcement, and companies—one that protects human rights, one that invades them—illustrates the difficult freedom of expression and privacy balancing act facing ICT companies today. This is essential context to keep in mind.

---

- 1) First, there are legitimate human rights reasons why governments, law enforcement agencies, and companies may restrict the free flow of information (such as removing images of child exploitation), or allow access to personal information (such as tackling fraud, terrorism, or violent crime). It is the duty of government to protect human rights; in that sense the majority of law enforcement activities are undertaken to protect human rights rather than violate them.

It is for this reason that enabling legitimate law enforcement agencies access to data or restricting certain types of information constitute important parts of a reasonable commitment to respecting human rights by ICT companies.<sup>2</sup>

- 2) Second, while these activities are frequently undertaken with positive public policy goals in mind, there is always the risk that governments and law enforcement agencies will make demands of the private sector to undertake privacy or freedom of expression-invasive activities that infringe on human rights. Incidents of this type will be small in number when compared to the overall volume of law enforcement; however, incidents of this type will be especially significant in terms of their impact on human rights.

It is for this reason that understanding why, how, and when to deny government access to data or demands to restrict content—and mitigate the risk of being asked in the first place—is a reasonable commitment by ICT companies to respect human rights.

The contrast between these two features of the relationships among national security, law enforcement, and companies—one that protects human rights, one that invades them—illustrates the difficult freedom of expression and privacy balancing act facing ICT companies today. This is essential context to keep in mind throughout this report.

### National and Local Context

A prominent feature relevant to how business may choose to navigate this difficult balancing act is the national and local context within which companies operate or provide products, services, and technologies. There are three variations in this context that are important in shaping a company's approach to protecting human rights:

- 1) Some governments are more transparent than others in how their national security and law enforcement priorities are pursued and the requirements that they place on the private sector to assist.
- 2) Some governments undertake national security and law enforcement activities that are consistent with their local domestic law, while other governments (to varying degrees) pursue national security and law enforcement activities that are in conflict with their own domestic law.
- 3) Some governments have in place legal frameworks that are consistent with internationally recognized laws and standards on human rights, while other governments (again, to varying degrees) have in place legal frameworks or pursue national security and law enforcement activities that are inconsistent with these international standards.

---

<sup>2</sup> *K.U. v. Finland*, European Court of Human Rights, 2 December 2008, <http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=843777&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649>



These national and local differences are documented by the OpenNet Initiative, which aims to investigate, report, and analyze the various internet filtering and surveillance practices around the world.<sup>3</sup>

### **Importance of Dialogue**

This report draws upon expert interviews and desk-based research, and reaches one main conclusion: It is only through in-depth, constructive, and collaborative efforts that bring together a wide diversity of governments, stakeholders, and companies from across the ICT value chain to discuss these issues that we will be able to fully comprehend how to protect freedom of expression and privacy online.

These multi-stakeholder discussions will be particularly significant to the protection of freedom of expression and privacy given the dynamic and rapidly evolving nature of the ICT industry. New ICT products, services, and technologies are introduced at a rapid pace and it can be a significant challenge for companies to understand where tomorrow's greatest human rights risks and opportunities will reside. Dialogue that brings together the diverse manufacturers, developers, sellers, and users of this ICT technology with their various stakeholders will greatly assist efforts to address this challenge.

---

<sup>3</sup> See [www.opennet.net](http://www.opennet.net) and *Access Controlled* (The MIT Press, 2010), edited by Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain.

## 2. Executive Summary

We live in a world today where vast Information and Communications Technology (ICT) infrastructures and extensive flows of information have become natural and unquestioned features of modern life. Rapidly growing online services—everything from social media to ecommerce and virtual collaboration—have come to define our day-to-day lives in ways unimaginable just a decade ago. This increasingly pervasive, unpredictable, and rapidly changing interaction between ICT and society brings with it a wide range of new human rights risk drivers and ethical dilemmas for companies in the ICT industry, especially for how to protect and advance freedom of expression and privacy online.

In order to understand the ICT industry's freedom of expression and privacy risk drivers, it is important to consider certain characteristics of the ICT industry that distinguish it from other industry sectors. These characteristics exist across five spheres and have significant implications for how to best protect and advance human rights in the industry:

- 1) **End user** – plays a significant role in the human rights impact of ICT
- 2) **Legal frameworks** – can move more slowly than ICT product and service development
- 3) **Jurisdictional complexity** – increasingly significant as information becomes global and data flows across borders
- 4) **Technological complexity** – new products and services are continually introduced, often with unpredictable consequences for human rights
- 5) **B2B relationships with enterprise and government customers** – with whom ICT companies often co-design products and services<sup>4</sup>

The ICT industry has been increasingly proactive over the past few years in defining approaches to protecting freedom of expression and privacy. For example, the Global Network Initiative provides direction and guidance to companies on how to respond to government demands to remove, filter, or block content, and how to respond to law enforcement agency demands to disclose personal information. These types of risk drivers will be relevant for companies that hold significant amounts of personal information and/or act as gatekeepers to content, primarily telecommunications services providers and internet services companies.

These approaches to protecting human rights online have been focused at the content level or on personal information itself. However, human rights risk drivers can also be found at the product/service functionality level. These risk drivers can arise, for example, through the requirement that certain types of ICT products, services, and technologies contain functionalities that allow for the removal, filtering, and blocking of content, or which enable easier surveillance and access to personal information by law enforcement agencies. These types of risk drivers will be relevant for companies that build the underlying ICT infrastructure through which information flows, such as network equipment manufacturers, cell phone companies, and security software providers.

---

<sup>4</sup> This analysis is adapted from [Big Business, Big Responsibilities](#) (Palgrave Macmillan, 2010) by Andy Wales, Matthew Gorman, and Dunstan Hope, pp. 87-102.

There are a number of different points across the ICT value chain in which governments can interact with private sector companies, sometimes at the level of content or personal information, and sometimes at the product or service functionality level. It is at these intersections between governments and ICT companies that the need to respect, protect, and advance human rights is most significant.

The main body of this report sets out these risk drivers across eight segments of the ICT industry:

- 1) **Telecommunications Services** – risk drivers include requirements to assist law enforcement agencies in investigations
- 2) **Cell Phones and Mobile Devices** – location-based services such as mapping or advertising can present new sources of security and privacy risks
- 3) **Internet Services** – companies can receive demands to remove, block, or filter content, or deactivate individual user accounts
- 4) **Enterprise Software, Data Storage, and IT Services** – companies hosting data “in the cloud” may increasingly be gatekeepers to law enforcement requests or provide service to high-risk customers
- 5) **Semiconductors and Chips** – hardware can be configured to allow remote access, which may present security and privacy risks
- 6) **Network Equipment** – where functionality necessarily allows content to be restricted or data to be collected by network managers
- 7) **Consumer Electronics** – pressure may exist to pre-install certain types of software to restrict access to content or allow for surveillance
- 8) **Security Software** – risk drivers may include increasing pressure to offer simpler means of unscrambling encrypted information

While there are certainly variations between different parts of the ICT industry, this report also demonstrates that there are common themes, such as responding to requests, demands, and legal requirements from governments and law enforcement agencies, or more demands to unscramble encrypted information. It also demonstrates that the ICT industry is one integrated whole, and that it is only by understanding how this integrated whole works together that the ICT industry and its stakeholders can most effectively protect human rights.

However, this report only begins to hint at various ways that ICT companies can mitigate these risks, and so it only completes the first half of the analysis required for ICT companies to effectively address these human rights risks. What is needed is a concerted effort, undertaken by the industry as a whole and its various stakeholders (including human rights groups, governments, investors, and academics) to explore how the human rights of freedom of expression and privacy can be most effectively protected in the context of legitimate law enforcement and national security activities.

This report concludes by highlighting four key topics that such a dialogue should address: relationships with governments; designing future networks; implementing due diligence; and engaging employees, users, and consultants.

### 3. Characteristics of ICT and Human Rights

In order to understand the ICT industry’s freedom of expression and privacy risks, it is important to consider certain characteristics that distinguish ICT from other industry sectors. These characteristics have significant implications for how to best protect and advance human rights in the industry, and they can be summarized across five spheres:

- 1) End user
- 2) Legal frameworks
- 3) Jurisdictional complexity
- 4) Technological complexity
- 5) B2B relationships with enterprise and government customers<sup>5</sup>

The characteristics of these five spheres point to the need for in-depth, constructive, and collaborative efforts that bring together companies, governments, and stakeholders to understand the unfolding relationship between human rights and ICT—especially as technology, data, and online communications become increasingly pervasive.

Sphere	Implications for Human Rights	Implications for ICT Companies
End User	<ul style="list-style-type: none"> <li>The role of the product or service end user in human rights is more significant in the ICT industry than other sectors. Whether exposing human rights abuses online, using the internet as a platform for political discourse, or having privacy rights violated, the end user plays a particularly significant role in the human rights impact of ICT.</li> <li>End users are increasingly innovating with ICT products and services in unexpected ways that may be beyond company control.</li> </ul>	<ul style="list-style-type: none"> <li>ICT companies need to be transparent with users about the privacy and freedom of expression features of products and services (such as restrictions placed on content, or notice that personal information could be shared with law enforcement agencies).</li> <li>When faced with demands from governments that may infringe on rights to privacy or freedom of expression, companies and end users may find a “common cause” to protect human rights.</li> </ul>
Legal Frameworks	<ul style="list-style-type: none"> <li>New technologies, products, services, and business models tend to be introduced much faster than laws can be enacted to regulate them. Regulatory processes often move more slowly than ICT product and service development.</li> <li>Governments around the world are making increasing demands—some positive and some negative—that impact human rights.</li> <li>Laws that are enacted for ICT can sometimes conflict with internationally recognized human rights to security, privacy, and freedom of expression.</li> </ul>	<ul style="list-style-type: none"> <li>In the absence of regulation establishing minimum standards, or in the face of ICT-related laws that can violate human rights, an increasing burden is placed on ICT companies to be proactive in their protection of privacy and freedom of expression.</li> <li>In situations where local law conflicts with human rights, companies may need—or be expected to—challenge the law and its implementation.</li> <li>Regulatory uncertainty or conflict between local law and international human rights standards can be barriers to private sector investment.</li> </ul>

<sup>5</sup> Table and analysis adapted from [Big Business, Big Responsibilities](#) (Palgrave Macmillan, 2010) by Andy Wales, Matthew Gorman, and Dunstan Hope, pp. 87-102.

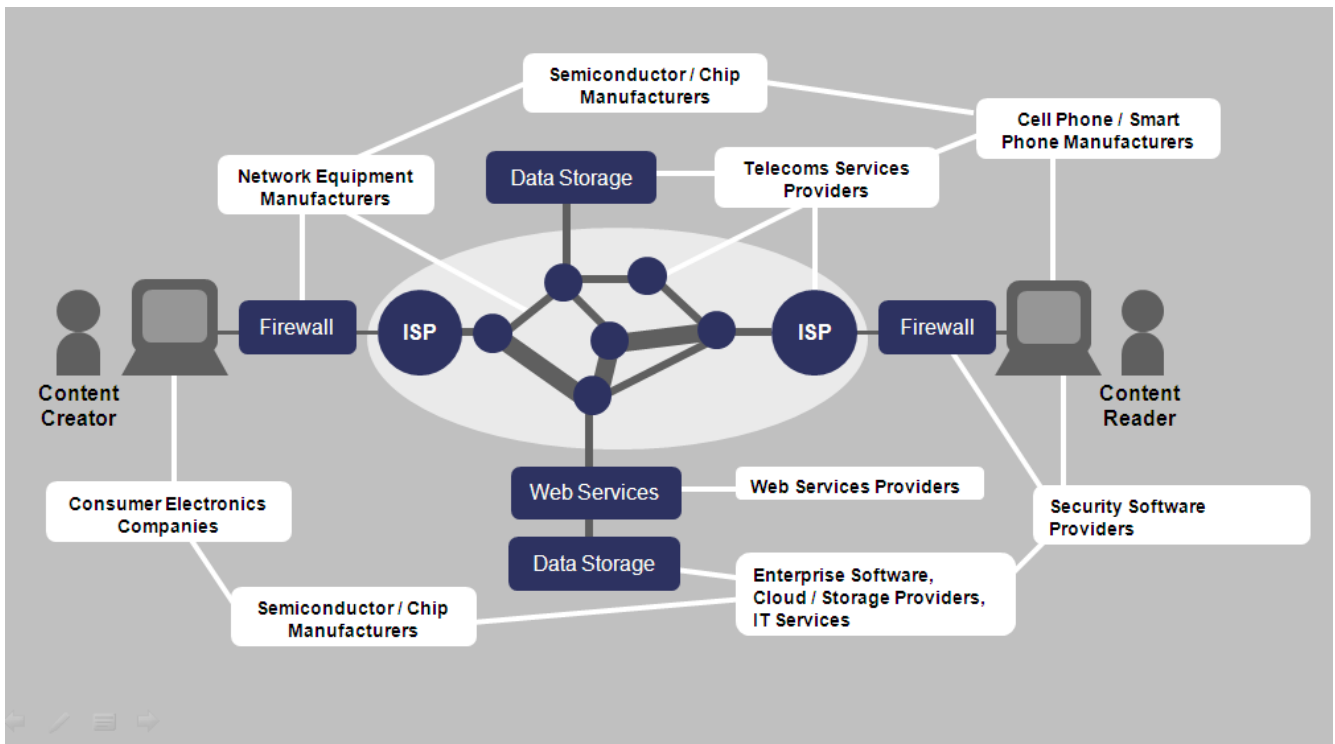
<p>Jurisdictional Complexity</p>	<ul style="list-style-type: none"> <li>• The internet is global, but laws and regulations governing ICT companies are often national.</li> <li>• The evolutions in ICT use are raising important questions about legal jurisdiction, especially as data flows across international borders, is stored in multiple jurisdictions, or can have different legal status in various jurisdictions. Human rights risks can vary according to which country personal information is stored in, and how a company's network is structured.</li> </ul>	<ul style="list-style-type: none"> <li>• When designing, architecting, and building networks, ICT companies need to be alert to the ways in which levels of human rights risk can vary among jurisdictions.</li> </ul>
<p>Technological Complexity</p>	<ul style="list-style-type: none"> <li>• New technology can be complex to understand, and new product functionalities are rapidly introduced.</li> <li>• New products and services bring new risks and opportunities all the time, sometimes with unpredictable consequences.</li> <li>• Rapid global communications can magnify the impact and significance of important events and incidents.</li> </ul>	<ul style="list-style-type: none"> <li>• Engagement between companies (which understand the technology, but less about its human rights impact) and stakeholders (who know less about the technology and more about possible human rights consequences) becomes more important. Improved shared knowledge and understanding grows in significance.</li> </ul>
<p>B2B and B2G: Relationships with Enterprise and Government Customers</p>	<ul style="list-style-type: none"> <li>• While ICT companies have little control over the actions of individual end users, they do have closer relationships with enterprise and public sector customers. ICT companies often co-innovate and co-design products and services with their major customers.</li> <li>• These enterprise and public sector customers can use ICT products, services, and technology for a variety of purposes—some good, some detrimental (known as the “dual use” dilemma).</li> </ul>	<ul style="list-style-type: none"> <li>• Undertaking market and customer due diligence—and understanding how the customer intends to use the ICT product—may be an increasing responsibility of ICT companies, which could be expected to enact strategies aimed at mitigating the risk of product misuse.</li> </ul>

## 4. ICT Industry Map

The ICT value chain is made up of many different yet interdependent parts. Understanding how these different parts interrelate as one overall ICT ecosystem is important to understanding human rights risk in the ICT industry.

However, the development of new technology and convergence between branches of the ecosystem that were previously considered separate make for a constantly evolving ICT industry map. To add to the complexity, a single company may be located in multiple parts of the ICT ecosystem, making it difficult for the company or its stakeholders to fully understand its key human rights risks.

Nevertheless, the different parts of the ICT value chain can be summarized in a simplified network diagram (below), which illustrates the relationship between these separate parts and the flow of information between a content creator and content reader. This can also be summarized in a table describing the different industry segments (next page).



ICT Industry Segment	Description	Illustrative Company List
Telecommunications Services	Providers of fixed and/or mobile telecommunications services to users, including both voice and data services (VoIP and traditional telecommunications network)	AT&T, China Mobile, China Unicom, Deutsche Telekom, France Telecom, Google, MTN, Reliance, SK Telecom, Skype, Sprint, Telefonica, TeliaSonera, Verizon, Vodafone
Cell Phones / Mobile Devices	Companies marketing, designing and manufacturing cell phones and mobile devices, over which a wide range of voice and data services (internet, email, SMS, etc.) can be accessed by users	Apple, Dell, HP, HTC, LG, Motorola, Nokia, Research In Motion, Samsung, SonyEricsson
Internet Services	Providers of a range of internet-based services, such as search, email, commerce, social networking, content, etc.	Adobe, Alibaba, Amazon, AOL, Baidu, eBay, Facebook, Google, IAC, Microsoft, Mozilla, News Corporation, Skype, Twitter, Yahoo!
Enterprise Software, Data Storage, and IT Services	Providers of a range of IT services to large and medium-sized businesses (including databases, cloud computing, storage, servers, virtualization, IT consulting, etc.)	BT, Dell, EMC, Fujitsu, Hitachi, HP, IBM, Microsoft, NEC, Oracle, Salesforce, SAP, Symantec
Semiconductors and Chips	Companies making the microprocessors, chipsets, integrated circuits, graphic chips, flash memory, and other components of computers, servers, mobile devices, cell phones, etc.	AMD, IBM, Intel, Qualcomm, Renesas, Samsung, Sony, STMicroelectronics, Texas Instruments, Toshiba
Network Equipment	Companies making fixed and wireless telecoms network equipment, such as switches and routers, and various network management services	Alcatel Lucent, Cisco, Ericsson, Fortinet, Hitachi, HP, Huawei, Juniper, NEC, NSN, Tellabs, ZTE
Consumer Electronics	Companies that design, market and manufacture various types of personal electronics equipment, such as computers, tablets, printers, gaming devices, TVs, DVD players, digital cameras, etc.	Acer, Apple, Best Buy, Cisco, Dell, HP, Lenovo, LG, Microsoft, Panasonic, Philips, Samsung, Sony, Toshiba
Security Software	Companies providing software that allows users and organizations to protect their information against external threats, or manage access to information (such as filtering, access controls, and blocking)	Fortinet, Intel (McAfee), Symantec, Websense

## 5. Freedom of Expression and Privacy Risk Drivers in the ICT Industry

---

Risk Drivers are the evolving features of the ICT landscape that result in specific risks to freedom of expression and privacy.

Risks result from the existence of these risk drivers in specific national, political, and law enforcement contexts.

---

The ICT industry has been increasingly proactive over the past few years in defining approaches to protecting freedom of expression and privacy. Many of these approaches have been focused *at the level of the content or personal information itself*. For example, the Global Network Initiative provides direction and guidance to companies on how to respond to government demands to remove, filter, or block content, and how to respond to demands to disclose personal information to law enforcement agencies. These types of risk drivers will be relevant for companies that hold significant amounts of personal information and/or act as gatekeepers to content (primarily telecommunications services providers and internet services companies).

However, human rights risk drivers in the ICT industry can also be found *at the product or service functionality level*. These risk drivers can arise, for example, through the requirement that certain types of ICT products, services, and technologies contain functionalities that allow for the removal, filtering, and blocking of content, or which enable easier surveillance and access to personal information by law enforcement agencies. These types of risk drivers will be relevant for companies that build the underlying ICT infrastructure through which information flows, such as network equipment manufacturers, cell phone/smart phone companies, and providers of security software.

Governments are increasingly aware of the distinction; media reports suggest that governments are contemplating “technology-neutral” regulations, which would require all types of products and services that enable communications to be technically capable of providing information required by law enforcement agencies.<sup>6</sup> Such requirements are already established as part of the ICT ecosystem with respect to the telecommunications services providers and the network equipment providers that supply to them. This further demonstrates that risks to the human rights of freedom of expression and privacy in the ICT industry—and associated risk-mitigation strategies—are not unique to internet companies, but are increasingly relevant to the entire ICT value chain.

### Features of the ICT Landscape

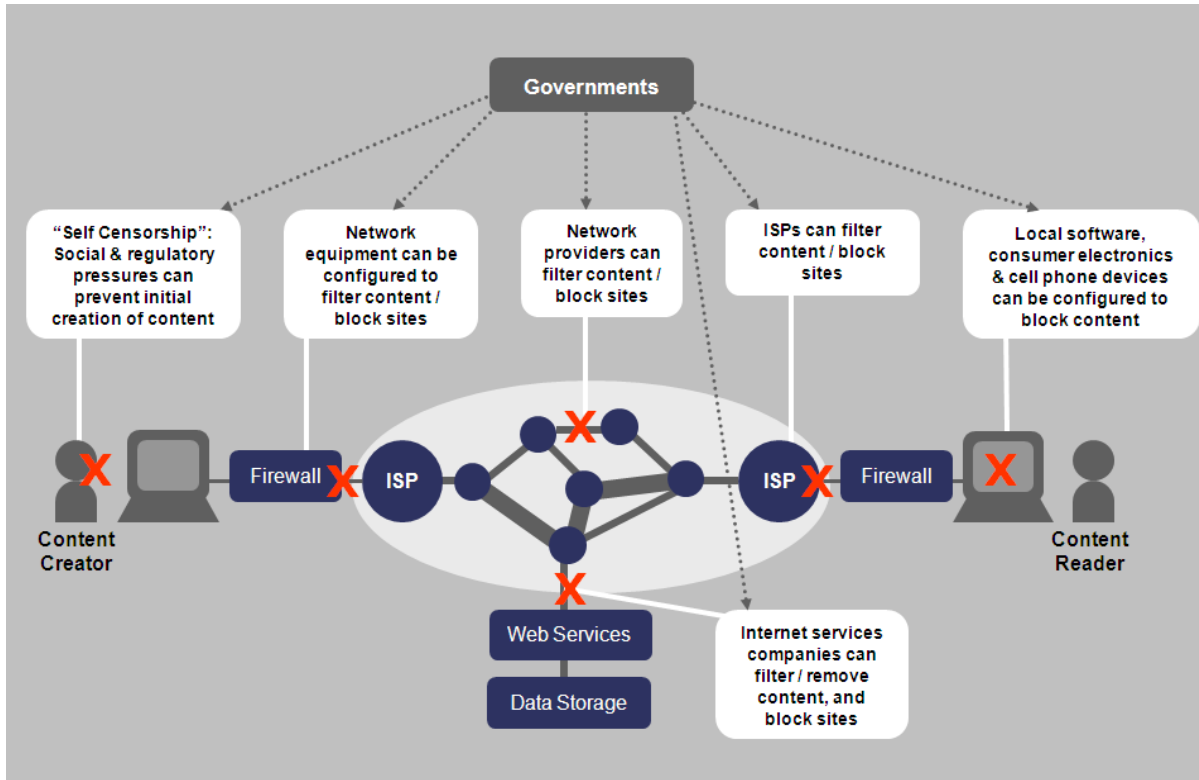
As can be seen from the accompanying diagrams, there are a number of different points across the ICT value chain in which governments can interact with private sector companies, sometimes at the level of content or personal information, and sometimes at the level of the product or service functionality. These links between companies and governments are highlighted because it is at these intersection points that the need to respect, protect, and advance human rights most often arises.

---

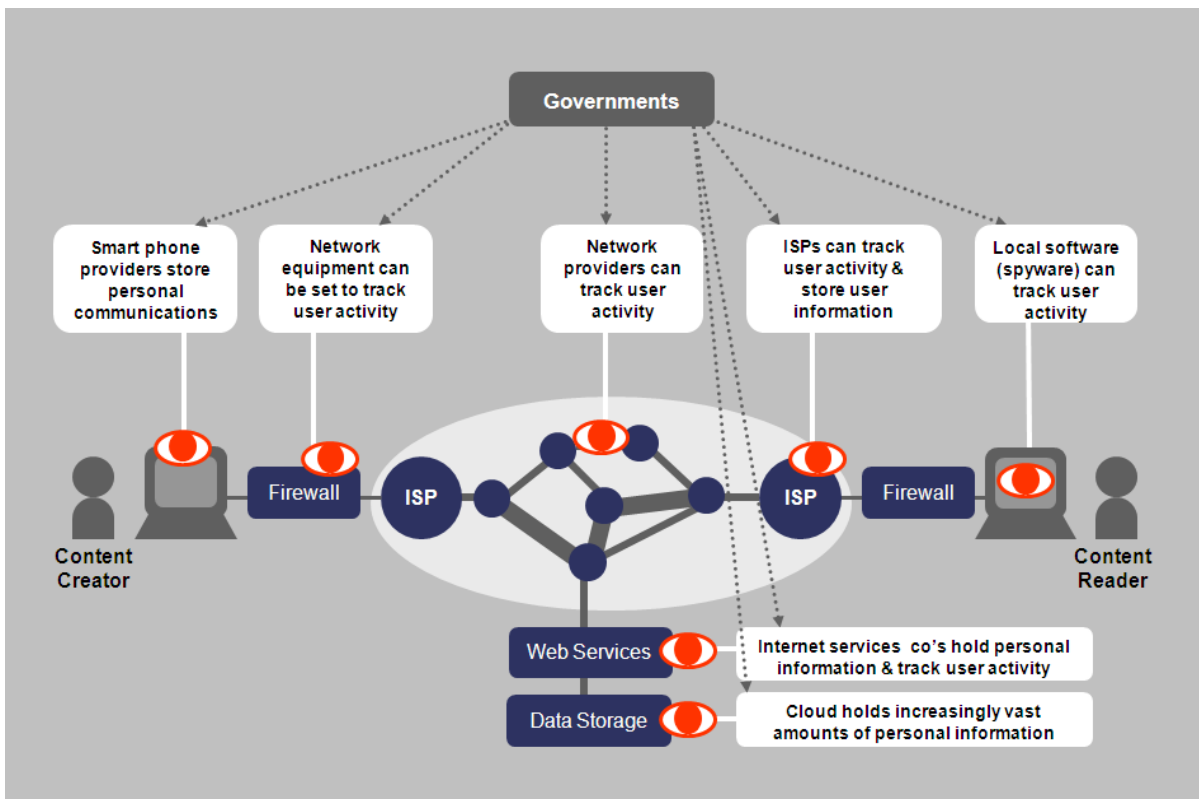
<sup>6</sup> *The New York Times*, “[US Tries to Make It Easier to Wiretap the Internet.](#)” Sept. 27, 2010.



## Freedom of Expression Risk Drivers Across the ICT Value Chain



## Privacy Risk Drivers Across the ICT Value Chain



## Summary of Human Rights Risk Drivers Across the ICT Value Chain

ICT Industry Segment	Key Freedom of Expression and Privacy Risk Drivers
Telecommunications Services	<ul style="list-style-type: none"> <li>• Companies hold vast amounts of personal information (call records, caller locations, etc.) and law enforcement agencies may demand access to it</li> <li>• Companies are often required to allow “lawful intercept” (real-time monitoring and surveillance, or the provision of analysis and evidence) for law enforcement agencies and governments</li> <li>• With the web increasingly accessed over mobile technology, telecom companies can become more involved in content restrictions. Telecoms can also be asked to block SMS messaging during events such as elections or protests.</li> <li>• Unlike internet services companies, telecom companies usually have a physical presence in the market, such as a physical network or sales offices. These features can increase the vulnerability of the company to “overbroad” law enforcement demands.</li> </ul>
Cell Phones / Smart Phones	<ul style="list-style-type: none"> <li>• Software/hardware can be configured to restrict access to certain online content, either at the discretion of the telecommunications network operator or mandated by government</li> <li>• Software/hardware designed to enable location-based services (such as mapping or advertising) can present freedom of expression and privacy risks when faced with certain types of law enforcement demands</li> <li>• Software/hardware functionality can be configured to allow law enforcement agencies access to user communications, which can sometimes be used for privacy-invasive purposes</li> </ul>
Internet Services	<ul style="list-style-type: none"> <li>• Internet services companies can receive demands from governments to remove, block, or filter content, or deactivate individual user accounts. This can be ongoing or event driven, such as during elections or protests.</li> <li>• Internet services companies can receive demands from governments to release personal information, such as emails, web surfing habits, etc.</li> <li>• There is pressure for internet companies to be held increasingly liable for user-generated content carried over their services (known as “intermediary liability”)</li> </ul>
Enterprise Software, Data Storage, and IT Services	<ul style="list-style-type: none"> <li>• Companies processing or hosting data in “the cloud” on behalf of users and customers may sometimes need to respond to law enforcement demands, and/or be asked to advise customers on how to respond to these law enforcement demands</li> <li>• Companies providing consulting advice alongside ICT hardware equipment (such as network equipment, consumer electronics, etc.) may need to advise enterprise or public sector customers on how to use the hardware in markets where government regulations infringe on human rights</li> <li>• Provision of IT services to certain customer segments (such as defense, national security, public safety, justice, law enforcement, etc.) in high-risk countries may increase risks that a company’s products and services are used in the violation of human rights</li> </ul>
Semiconductors and Chips	<ul style="list-style-type: none"> <li>• Hardware can be configured to allow law enforcement access for surveillance</li> <li>• Trends toward integrating security features at the chip level potentially increase the likelihood that governments will demand functionality that enables remote access by law enforcement agencies</li> </ul>

Network Equipment	<ul style="list-style-type: none"> <li>• Network managers may use functionality designed into networking equipment (such as network management and security capabilities based on filtering) to restrict certain categories of data, websites, and content</li> <li>• Network managers may use functionality designed into networking equipment (such as “deep packet inspection” and lawful intercept capabilities that provide for the collection and analysis of data) to allow access by governments to personal information and communications for use in law enforcement activities</li> </ul>
Consumer Electronics	<ul style="list-style-type: none"> <li>• Governments could demand that computer manufacturers pre-install filtering and/or monitoring software designed to restrict access to content and/or allow for surveillance</li> </ul>
Security Software	<ul style="list-style-type: none"> <li>• Filtering software can be used by governments and/or other companies to restrict content in ways that infringe on rights to freedom of expression</li> <li>• Governments could demand that filtering software restricting freedom of expression is pre-installed in computers and/or mobile devices</li> <li>• Provision of security software to certain customer segments (such as defense, national security, public safety, justice, law enforcement, etc.) in high-risk countries may increase risks that a company’s products and services are used in the violation of human rights</li> <li>• Governments may prohibit the use of strong forms of encryption or demand that companies offer simpler means for encrypted information to be unscrambled</li> </ul>

### Telecommunications Services

The human rights risk drivers for telecommunications services companies mainly relate to the vast amounts of personal information they hold—everything from call records to the caller’s location—which law enforcement agencies can demand access to. This access can be at a single moment in time or, in the case of real-time monitoring and surveillance, continuous and over an extended period of time. While most law enforcement activity is legitimate, companies can face demands from law enforcement agencies to hand over personal information in ways that may lead to human rights violations. And as has recently become evident in Egypt, telecommunications services companies can also come under significant pressure to restrict or take down their services.

While most of these risk drivers are a significant focus for internet services companies too, there are three distinguishing features inherent to the telecommunications services industry:

- **Telecommunications companies have substantial in-country presence: in addition to local employees there is the telecommunications network itself.** Internet services companies can often target services at a country (for example, services offered in the local language) while locating key assets such as servers, user data, and personal information in lower-risk locations. This flexible approach allows internet services companies to argue that their information and equipment falls under the domain of a different jurisdiction. However, this is not true for telecommunications companies. In order to offer a local service they also need to build an extensive telecommunications network in that country or partner with a firm who has built such a network. Such networks usually represent billions of dollars of investment requiring a return. The existence of this network clearly brings them under the local

jurisdiction and thus increases their vulnerability to overbroad law enforcement demands that may infringe human rights.

- **Telecommunications companies often have close relationships with state entities.** In order to provide a local service, a telecommunications company will usually have to establish close relationships with local state entities. This can be in the form of the local license that the service provider requires in order to provide service, or a joint venture with a current or former state-owned enterprise. Both these scenarios increase the risk that, either for legal reasons (conditions in the local operating license) or simply because of historical local practice (current and former state-owned enterprises will likely have a deeply ingrained culture of collaboration with law enforcement agencies), the telecommunications company collaborates too closely with law enforcement agencies. This presents a risk to human rights in cases in which the government, or specific government actions, may be associated with human rights violations.
- **Access to communications (including the internet) over mobile devices is expanding rapidly in emerging markets, which are often the very same places where human rights risks are higher.** In developing and emerging markets, mobile phones are increasingly becoming the main channel through which users will access the internet. Given the sheer numbers of potential customers in these markets, which are often ones in which greater human rights risks are located, this represents a substantial increase in the scale of human rights risk.

### Cell Phones and Mobile Devices

As cell phones become smarter, richer in features, and increasingly used as a gateway to the internet, human rights risks grow for companies who market and manufacture cell phones and mobile devices:

- **Software and hardware functionality designed to enable location-based services** – These are services (such as mapping or advertising) based on the service provider knowing where the customer is at any given moment in time. These capabilities present new and challenging privacy and security risks, such as in cases in which law enforcement agencies inappropriately seek the location of a user. These risks potentially impact every participant in the mobile ecosystem—handset makers, providers of operating system software, application providers, and telecommunications service providers. Each face decisions that impact user privacy.
- **Software and hardware functionality enabling access by third parties** – Cell phones and mobile devices form part of the overall ICT infrastructure that can be designed and configured to more easily enable access by law enforcement agencies. While the functionality itself can be considered human rights neutral (there can be good reasons to allow law enforcement access to personal information and communications), the functionality could be misused in ways that may cause companies to be inadvertently or intentionally associated with privacy-invasive activities.
- **Software and hardware functionality enabling content restrictions** – As smart phones become an important access point to the internet, so the risk increases that certain governments may seek ways to impose content restrictions at this level.

## Internet Services

The freedom of expression and privacy risk drivers faced by internet services companies have been well documented by organizations such as the Global Network Initiative and the OpenNet Initiative. Broadly speaking, internet services companies can receive demands from governments to remove, block, or filter content, or to release personal information, such as email records and web surfing habits. Two recent trends of particular relevance to human rights merit emphasis here:

- ***Internet services companies can receive requests and demands to deactivate user accounts.*** Online services, such as email, social networking sites, video communities, and blogs, are important tools for citizen journalists, political campaigners, and human rights advocates to express their points of view and to organize movements. However, companies can come under pressure—from governments and users who may object to certain content—to deactivate accounts and take down content, especially during key events such as elections or protests.
- ***Some policymakers believe that internet services companies should be made liable for user-generated content that is carried over their services, such as blogging sites or video hosting.*** Policies creating liability for carriers of content sent or created by users can be threats to 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 restraints on speech.

## Enterprise Software, Data Storage, and IT Services

As the trend toward cloud computing continues and IT services companies increasingly co-create and co-innovate new products and services with their larger customers, companies that provide enterprise software, IT services, databases, cloud computing, data storage, servers, virtualization, and IT consulting are faced with a number of growing human rights risk drivers:

- ***Responding to demands from law enforcement agencies*** – Companies processing or hosting data in “the cloud” on behalf of users and customers may increasingly be the gatekeepers to law enforcement demands. It is often the case that when ICT companies process or store data in the cloud their approach to security and privacy—including how to respond to law enforcement demands—will be governed by the customers rather than the ICT company. In other words, it is often the client, rather than the ICT company, that is the main entity facing the risk driver. However, as the gatekeeper to the information, the company is in a position to advise customers on best practices from a human rights perspective. Moreover, governments seeking data may not recognize distinctions between an ICT company providing technical platforms for data hosting and the client who manages the data; they will seek data from either or both parties. Also, the trend toward cloud computing raises a range of jurisdictional issues, such as which governments are entitled to compel disclosure when user data is stored in a country other than their own or in two countries at the same time. With cloud computing, ICT companies may increasingly find themselves at the receiving end of demands for personal information from governments.
- ***Providing consulting advice on how ICT hardware and software is used*** – ICT companies providing equipment, IT services, data storage and

enterprise software may not always provide simple off-the-shelf hardware and software. They often provide consulting advice alongside ICT hardware (such as network equipment, databases, computing equipment, etc.) and guidance on how the hardware and software can be used for maximum value. There is a need therefore to provide consulting advice consistent with the human rights of privacy and freedom of expression, especially to customers in higher-risk jurisdictions.

- ***Provision of services to high-risk customers in high-risk locations*** – A number of freedom of expression and privacy risk drivers can arise when ICT companies provide enterprise software, data storage, and IT services to high-risk customer segments (such as defense, national security, public safety, justice, law enforcement etc.) in high-risk countries. Without effective due diligence relating to the country/market and the specific customer, such companies run the risk of being associated with human rights violations.

### **Semiconductors and Chips**

Companies that design and manufacture semiconductors and chips make choices about product functionality and default settings that have potential implications for human rights. However, these functionalities also take us into an ethical grey zone: For example, the same chip-level functionality that allows remote access to a PC for maintenance and troubleshooting has potentially more negative applications too, such as surveillance. There are two other recent developments that also present human rights risk at this level: the pressure from governments to configure chips in such a way that back-door access to ICT networks is more easily obtained, and the potential trend toward embedding security features usually provided at the software level (see below) into the chip.

### **Network Equipment**

The increasing pervasiveness of ICT in all countries requires ever more extensive networks capable of carrying larger and larger amounts of data in increasingly sophisticated ways. There are three main risk drivers for companies providing fixed and wireless network equipment, such as switches and routers, and various network management services:

- ***Providing product functionality that enables censorship and content restrictions*** – Networking products and technologies (such as switches and routers) have functionality designed to allow network managers restrict certain categories of data, websites, and content. Network management and security capabilities based on filtering are critical to mitigating attacks on the network and are essential to enabling the reliable flow of information—the internet would collapse without these features. There can also be very good reasons to provide functionality that allows the blocking of certain content, such as child exploitation. However, used by certain customers in particular ways—for example, restricting access to a broader range of information, such as political content—could cause network equipment suppliers to be associated with restrictions to the human right of freedom of expression.
- ***Providing product functionality that enables privacy-invasive activities by law enforcement agencies*** – Networking products and technologies also contain functionalities (such as “deep packet inspection” and “lawful intercept capabilities”) designed to allow access by third parties to personal information and communications. While the functionality itself can be considered human rights neutral (there can be good reasons to allow access to personal information and communications, such as legitimate law enforcement), usage by certain customers in particular ways could cause

network equipment suppliers to be associated with privacy and security-invasive activities. It should be noted that network equipment suppliers are often mandated to provide this functionality as a requirement set by the telecommunications operator buying the equipment; in turn the telecommunications operator will have inserted this requirement as a license condition established by the government or regulator. It should also be noted that these requirements exist in all markets, and equipment suppliers find it difficult to take a “double standards approach” by offering that functionality in some markets and not others.

- ***Providing consulting advice on how ICT hardware and software is used***  
– While the provision of off-the-shelf hardware at the request of customers or governments raises debatable ethical questions over whether or not a company is considered complicit in a human rights violation, these ethical questions are more clear in the case of the consulting advice provided alongside the equipment. If companies advise enterprise or public sector customers on how to use networking products in ways that restrict freedom of expression or invade privacy and security, then the company would be more closely associated with these human rights abuses.

## **Consumer Electronics**

Consumer electronics companies provide a range of products such as computers, tablets, printers, gaming devices, TVs, DVD players, digital cameras, etc. An increasing number of these devices are linked to the internet.

Here the recent “Green Dam, Youth Escort” proposals in China provide an illustration of the human rights risk drivers that may increasingly exist for consumer electronics companies. Made public in June 2009, these proposals would have required computer manufacturers selling in China to pre-install filtering software designed to restrict access to undesirable content. Testing of the software found that it blocked content well in excess of what might be deemed reasonable (such as child exploitation sites) to include religious sites, human rights content, and political themes. The software also had surveillance and privacy-invasive capabilities, such as including the ability to terminate word processing and email programs when a content algorithm detected inappropriate speech.<sup>7</sup>

Though subsequently defeated by both international and domestic opposition, the existence of this demand from government provides an early indication of the nature of human rights risk drivers that may exist for providers of personal systems equipment in years to come. For example, recent stories have emerged raising the possibility of Green Dam-like requirements in Indonesia and Vietnam (monitoring software is already required to be installed on computers at all internet cafes, hotels, and other establishments in Hanoi).<sup>8</sup>

## **Security Software**

Security has become a progressively more significant feature of the ICT ecosystem. With increasingly large amounts of information stored online, it is perhaps inevitable that the number of people attempting to access that

---

<sup>7</sup> See the OpenNet Initiative report, “China’s Green Dam: The Implications of Government Control Encroaching on the Home PC,” at <http://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc>

<sup>8</sup> IDG News Service, “Activists Worry About a New ‘Green Dam’ in Vietnam,” June 4, 2010: <http://www.nytimes.com/external/idg/2010/06/04/04idg-activists-worry-about-a-new-green-dam-in-vietnam-51678.html>

information without authorization has also grown substantially—and with that, the demand for increasingly sophisticated security software.

- **Encryption capabilities may become a battleground between governments and companies.** With the increasing importance of information security, the use of encryption technology to protect communications is growing in significance. Governments and companies have long had discussions regarding the commercial deployment of strong encryption, which is considered essential for e-commerce, information security, and user privacy. However, recent developments suggest that governments around the world may more frequently demand the means to easily unscramble encrypted communications. While the human rights risk of such access may be small in some jurisdictions, it could become much greater in countries with poor human rights records.
- **Filtering software can be used by governments and/or other companies to manage content restrictions at the country level.** Security software companies face risks that their products are: 1) misused by customers in ways that violate agreed terms of service; or 2) reverse engineered in ways that allow their misuse.
- **Governments could demand that filtering software is pre-installed in computers and/or mobile devices.** As highlighted above, while the recent “Green Dam, Youth Escort” proposals failed, they did shed light on a potential future trend: requirements from governments that filtering (and potentially, surveillance) software is pre-installed in computers and mobile devices. In this scenario, security software companies will be faced with a decision of whether to put themselves forward as providers of this software or to decline based on their potential complicity with human rights concerns. There are a range of factors that may influence a decision here, including the nature of the government and the amount of choice made available to users over whether they install the software or not.
- **Provision of products and services to high-risk customers in high-risk locations.** A number of freedom of expression and privacy risks could arise if security software companies provide products and services to high-risk customers (such as defense, national security, public safety, justice, law enforcement, etc.) in high-risk countries. Without effective due diligence relating to the country/market and the specific customer, such companies run a risk of being associated with human rights violations.



## 6. Conclusions

---

What is needed now? A concerted effort, undertaken by the ICT industry and its various stakeholders (including human rights groups, governments, investors, and academics), to explore how the human rights of freedom of expression and privacy can be most effectively protected in the context of legitimate law enforcement and national security activities.

---

This report describes how companies across the ICT value chain could face particular human rights risks. While there are certainly variations between different parts of the ICT industry, this report also demonstrates that there are common themes, such as responding to requests, demands, and legal requirements from governments and law enforcement agencies, or the increasing challenge of demands to unscramble encrypted information. It also demonstrates that the ICT industry is one integrated whole, and that it is only by understanding how this integrated whole works that we can most effectively protect human rights.

However, this report only begins to look at various ways that ICT companies can mitigate these risks; thus, it only completes the first half of the analysis required for ICT companies to effectively address the human rights risks of freedom of expression and privacy. What's needed now is a concerted effort, undertaken by the industry as a whole and its various stakeholders (including human rights groups, governments, investors, and academics) to explore how the human rights of freedom of expression and privacy can be most effectively protected in the context of legitimate law enforcement and national security activities.

The Global Network Initiative (GNI) resulted from an 18-month process of learning, dialogue, and collaborative drafting to fully understand how participating companies could most effectively reduce human rights risk. A tremendous amount was learned during this time and it was only as a result of such dialogues that the GNI and the various solutions it provides could be launched. This report raises many new questions and issues that would benefit from similar dialogues involving the remainder of the ICT industry.

There are four key topics that such dialogue should address: 1) relationships with governments; 2) designing future networks; 3) implementing due diligence; and 4) engaging employees, users, and consultants.

### Relationship with Governments

Governments play critical roles in the human rights profile of ICT companies. Through various law enforcement and national security activities, governments establish the essential context within which the human rights impacts of ICT companies are felt. The role of government also raises a huge dilemma for the ICT industry: Many law enforcement activities are undertaken for the right reasons and to protect human rights, but some are not. Given that, what approach should ICT companies take to navigate relationships with governments all over the world on the topics of freedom of expression and privacy?

A dialogue among more ICT companies could usefully address this question and define industry-wide approaches and expectations. Some key aspects include:

- Are there ways for ICT companies to work with governments and stakeholders to define product functionalities and standards that enable legitimate law enforcement activities yet limit the risk of abuse?
- How can companies work together with governments to shape approaches to human rights and law enforcement online that more effectively protect human rights?

---

The role of government also raises a huge dilemma for the ICT industry: Many law enforcement activities are undertaken for the right reasons and to protect human rights, but some are not. Given that, what approach should ICT companies take to navigate relationships with governments all over the world on the topics of freedom of expression and privacy?

---

- Can companies and stakeholders increase the level of understanding and sophistication that exists in governments all over the world on how to maximize the human rights benefits of ICT?

It is significant to note that the next three to five years represent an important period of time during which the global governance of the internet will become much clearer. Various norms building processes and bodies, such as the Internet Governance Forum, are likely to establish new regional and international frameworks relevant to privacy and freedom of expression online. It will be important for those with an interest in protecting human rights in the digital age to be active participants in these processes and to have shared opinions on which to base their participation.

### Designing Future Networks

The private sector designs ICT networks under considerable influence from governments and law enforcement agencies. For example, manufacturers of telecommunications equipment build “lawful intercept” capabilities into their equipment at the request of telecommunications services providers, who in turn are making that request to meet licensing conditions established by governments. However, there is room for governments, stakeholders, and ICT companies to address the following questions:

- To what extent can the functionality of new ICT products be designed to minimize censorship or illegitimate access to personal information, while allowing for legitimate law enforcement activities?
- 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 interdependent network?

### Implementing Due Diligence

The dual-use nature of ICT networks and law enforcement—that both can be used to protect the public good and to do harm—increases the significance of approaches to due diligence by companies. Indeed, the concept of human rights due diligence forms a key part of the approach advocated by the UN Special Representative on Human Rights in his recommendation on how private sector actors can take responsible approaches on human rights. Important questions for the ICT industry and its stakeholders include:

- How can ICT companies assess the risk that customers (i.e. government clients or enterprises) 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)? Are there certain customers (e.g. public security customers in certain high-risk locations) that an ICT company may choose not to sell to? How can a company decide? Due diligence at the level of the market will be especially important for telecommunications companies, which need to make huge investments before entering a country and have very little room for maneuver once they are there.

---

The dual-use nature of ICT networks and law enforcement—that both can be used to protect the public good and to do harm—increases the significance of approaches to due diligence by companies. Indeed, the concept of human rights due diligence forms a key part of the approach advocated by the UN Special Representative on Human Rights in his recommendation on how private sector actors can take responsible approaches on human rights.

---

- 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 yet unethical, or which may be invasive of privacy and freedom of expression?

### **Engaging the Employees, Users, and Consultants**

The role of business in protecting human rights in the ICT industry can be complex and unpredictable. There are all sorts of people who use ICT—for instance: end users innovating with new ICT products and services; company employees devising tailored solutions for enterprise and public sector customers; and consultants trained in various hardware or software applications advising client organizations on how to make the most ICT.

This diversity raises interesting questions about the potential responsibility of companies to inform and train users, employees, and consultants in the intended use of ICT and the human rights implications of this use. It also highlights the urgent need to raise awareness and fluency among the user population about the human rights risks and opportunities of ICT products and services.

- 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 an ICT company have if the advice about the use of its products is provided by independent contractors, who may not have been trained by the company?
- How can ICT companies provide transparent communications with users about the privacy and freedom of expression risks associated with their online presence?

Similarly, it will be important to continue the development of two new communities of experts that are emerging at the intersection of ICT and human rights: communities inside ICT companies much more familiar with human rights issues than in the past, and communities inside human rights organizations much more familiar with the implications of new technology than in the past. With ICT increasingly pervasive in 21st-century society, deeper interaction between these two communities—at local, national, and international levels—will be critical for our collective ability to protect freedom of expression and privacy in the digital age.

# Global Network Initiative

[www.globalnetworkinitiative.org](http://www.globalnetworkinitiative.org)

Inaugural Report 2010

**Our work.**

**Our vision.**

**Our progress.**





# TABLE OF CONTENTS

GNI Members . . . . . **1**

Message From GNI Executive Director Susan Morgan . . . . . **2**

Human Rights and ICT: An Evolving Landscape . . . . . **3**

GNI: Governance and Work . . . . . **7**

GNI: Creating Accountability and Transparency . . . . . **10**

GNI: Driving Change . . . . . **13**

GNI: Lessons Learned and Looking to the Future . . . . . **23**

## GNI MEMBERS

The Global Network Initiative (GNI) benefits from the active involvement of a broad range of participants, including companies in the information and communications technology (ICT) sector, civil society organizations (including human rights and press freedom groups), investors and academics. Our current members are:

### ICT Companies

Google  
 Microsoft  
 Yahoo!

### Civil Society Organizations

Committee to Protect Journalists  
 Center for Democracy & Technology  
 Electronic Frontier Foundation  
 Human Rights in China  
 Human Rights First  
 Human Rights Watch  
 IBLF  
 Internews  
 United Nations Special Representative to the Secretary-General on Business & Human Rights (Observer Status)  
 World Press Freedom Committee

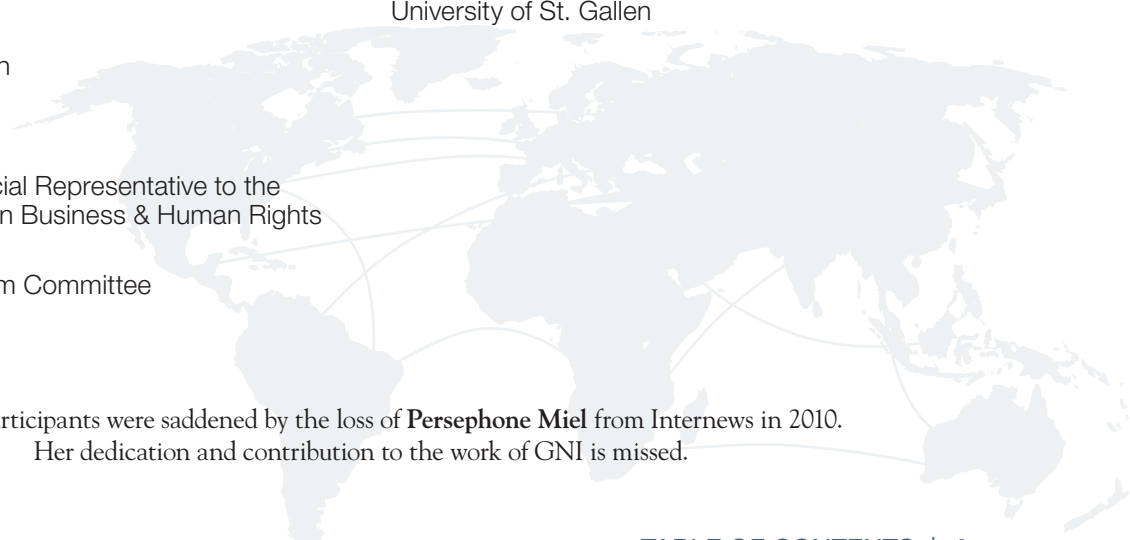
### Investors

Boston Common Asset Management  
 Calvert Group  
 Domini Social Investments  
 F&C Asset Management  
 Trillium Asset Management

### Academics and Academic Organizations

The Berkman Center for Internet & Society at Harvard University  
 Deirdre Mulligan, U.C. Berkeley School of Information  
 Ernest Wilson, Annenberg School for Communication & Journalism, University of Southern California (*personal capacity*)  
 Rebecca MacKinnon, New America Foundation (*personal capacity*)  
 Research Center for Information Law, University of St. Gallen

All GNI participants were saddened by the loss of **Persephone Miel** from Internews in 2010. Her dedication and contribution to the work of GNI is missed.



# MESSAGE FROM GNI EXECUTIVE DIRECTOR SUSAN MORGAN

The Internet and related communications technologies have tremendous potential for furthering the public good. They can lower the cost of market entry for businesses; enable access to knowledge in developing countries; and transform access to healthcare – the benefits can be huge and often unanticipated. Information and communications technologies (ICTs) can provide ordinary people everywhere with unprecedented opportunities to create, share and access information and content worldwide.

But as ICTs become ubiquitous in daily life, the impact of technology policy on fundamental human rights and civil liberties grows. Governments have responsibilities to address national security concerns, uphold laws and protect children online. Additionally, governments are responsible for upholding the internationally recognized human rights of their citizens. But in addressing legitimate issues, governments are increasingly asking companies in the ICT sector to take actions that could undermine the free expression or privacy rights of their users. Some governments make demands of the ICT sector that are related to suppressing political activity and which infringe human rights. Moreover, governments are not monolithic. Government actions focused on both legitimate and illegitimate objectives can arise within the same country. Among the foremost current challenges for governments is discharging the wide range of responsibilities for which they are accountable, while respecting human rights.

ICT companies are at the forefront of this challenge. Of course, ICT companies have an obligation to comply with lawful government demands, and ICT companies can and should play a role in addressing legitimate concerns such as cybercrime, national security and the safety of children online. But ICT companies also have a responsibility – rooted in internationally recognized human rights standards – to respect the free expression and privacy rights of their users. When ICT companies receive government demands that effect such rights, tension can arise between these two responsibilities.

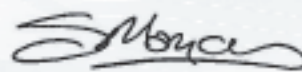
In this complex environment, there is a clear role and responsibility for civil society, academia and the investor community. Governments and ICT companies need good guidance, grounded in internationally accepted standards, and some degree of political consensus, in order to fashion responses to these challenges. By contributing analysis, expertise and perspective, civil society organizations, academia and investors support both ICT companies and governments, as they further security and law enforcement goals in a manner that protects and advances human rights.

GNI was created to address these issues. The GNI Principles,<sup>1</sup> Implementation Guidelines,<sup>2</sup> and Governance, Accountability & Learning Framework<sup>3</sup> provide substantive and operational guidance to ICT companies regarding how to respond to government policies and practices in a manner that protects and advances freedom of expression and privacy.

GNI members benefit from:

- real-time problem-solving support from fellow GNI members with deep expertise and/or on-the-ground knowledge and networks
- an accountability framework that establishes the credibility of the process of implementing GNI's Principles and cultivates trust in GNI member company actions
- a unique platform for shared learning and collaborative public policy engagement.

In this inaugural report, we showcase the initial work of our members, consider the trends since GNI launched in 2008, and set forth our future vision. GNI is a collaborative effort, and the diversity of its membership is its greatest strength. As GNI's first Executive Director, I welcome and encourage greater participation, constructive criticism and growing membership. I invite you to join our ambitious and essential effort to protect and advance free expression and privacy in the ICT environment.



Susan Morgan

1. <http://www.globalnetworkinitiative.org/principles/index.php>.  
 2. <http://www.globalnetworkinitiative.org/implementationguidelines/index.php>.  
 3. <http://www.globalnetworkinitiative.org/governanceframework/index.php>.

# HUMAN RIGHTS AND ICT: AN EVOLVING LANDSCAPE

The human rights and ICT landscape extends across not only the diversity of companies within the ICT sector, but also the growing variety of issues that place ICT companies in positions where they must wrestle with impacts on human rights such as censorship or surveillance. One of the ways in which GNI responds is by developing approaches that private sector actors can take to promote respect for human rights in light of government policies or practices that implicate free expression and privacy. GNI is guided in this by the diverse expertise of its members.

GNI was formed as a result of a groundswell of interest in two issues: (1) governments compelling online service companies to disclose personal data about their users in order to enforce laws against political activity, and (2) governments limiting access to information by removing it from search results, blogs and other online sources. In the early discussions that led to the creation of GNI, examples involving China dominated the headlines. Now, with rapid development in the industry, many new issues are emerging globally. For example:

- Governments increasingly link cyber-security to national security. This prompts consideration of the free expression and privacy implications of policy development in national security and law enforcement. Government policies on cyber- and national security may place ICT companies in

between security objectives and the privacy rights of users, including human rights activists, journalists and others who may be particularly at risk.

- Internet censorship is a rising trend, with approximately 40 countries<sup>4</sup> filtering the Web in varying degrees, including democratic and non-democratic governments. Governments are using more sophisticated censorship and surveillance techniques, including blocking social networks, to restrict a variety of types of content, including content that is legally restricted (e.g., drugs) or culturally sensitive (e.g., related to sexuality), or that implicates national security matters.<sup>5</sup>
- Recent legislation and regulation around the world is calling intermediary liability protections into question for Internet service providers, search engines, blog hosts and other intermediaries.<sup>6</sup> Even in countries that protect intermediaries from content liability, ICT companies are nonetheless often under pressure to police content published on their networks and platforms. In some jurisdictions, vague and/or overbroad content restrictions encourage self-censorship and other restrictions on online speech in order to minimise the financial and legal risk for intermediaries.
- Deactivating accounts and removing content on social networking and other sites presents a growing set of issues. In some cases, these

**“In a world where the Internet is rapidly becoming the critical medium to ensure respect for human rights, complying with the Principles of GNI is an opportunity for companies to ensure that they are a part of this trend and reduce the risk that they undermine it.”**

— Arvind Ganesan, Director of Business and Human Rights, Human Rights Watch

4. See <http://opennet.net/research/profiles>.

5. According to a new book from the OpenNet Initiative: [F]irst-generation controls, typified by China’s “Great Firewall,” are being replaced by more sophisticated techniques that go beyond mere denial of information and aim to normalize (or even legalize) a climate of control. These next-generation techniques include strategically timed distributed denial-of-service (DDoS) attacks, targeted malware, surveillance at key points of the Internet’s infrastructure, take-down notices, and stringent terms-of-usage policies. Ronald J. Deibert, John G. Palfrey, Rafal Rohozinski and Jonathan Zittrain (Eds.), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (2010) (<http://www.access-controlled.net/>).

6. [http://www.globalnetworkinitiative.org/issues/Intermediary\\_Liability.php](http://www.globalnetworkinitiative.org/issues/Intermediary_Liability.php).



practices represent a form of censorship. And even where they are carried out for reasons like enforcement of abuse and security policies, specific risks for human rights activists (and negative implications for the rights they seek to protect) have nonetheless arisen.

- The issues surrounding WikiLeaks not only underscore the need for companies to consider the human rights implications of the business decisions they take, but also show how the situations confronting companies are constantly evolving.

GNI's approach developed within a framework of international human rights. Our vision is to protect free expression and privacy rights in the context of today's and tomorrow's information technology environment. That context is extraordinarily complex.

The ICT sector includes networks, hardware, software, content and diverse services. Within this sector, many businesses are built and operated by the private sector; others are entirely or partially state-owned; still others may have been initially created by the state and then privatized (especially telecommunications). Aspects of ICT industry operations may require heavy in-country investment and a considerable presence in each market; others may require neither.

Compounding this complexity are the following factors: (a) the fast pace of innovation of Web 2.0 products, services and technologies (web-based services accessed via the Internet regardless of device), (b) the flow of huge amounts of data across borders, and (c) the storage of data in multiple jurisdictions. Against this backdrop, and given the pace of technological advances, creating law and policy in a timely way is especially challenging.

These complexities and challenges have not escaped the media's attention. The free expression and privacy dimensions of issues arising in the ICT

**“GNI has an important role to play in ensuring that IT companies not only voice their support for online freedom of expression but actually take concrete steps to avoid being the accomplices of censorship or the online surveillance of dissidents by law enforcement officials.”**

**— Lucie Morillon, Head of New Media Desk, Reporters Without Borders**

landscape are increasingly subject to media scrutiny. Here are some descriptions, drawn from media reports, of notable issues:

- China's Ministry of Industry and Information Technology proposed in 2008 that personal computers sold in China must run software called “Green Dam Youth Escort.”<sup>7</sup> In addition to blocking access to blacklisted websites, the Green Dam software collects personal data about users. As the BBC and other news outlets reported, the proposal for mandatory pre-installation has been suspended,<sup>8</sup> but some computer makers are voluntarily complying, and public Internet facilities (e.g., Internet cafes) run the software.<sup>9</sup>
- In April 2010, the People's Committee of Hanoi in Vietnam followed China's example and required installation of monitoring software on all computers in public Internet facilities.<sup>10</sup>
- Mobile is already a popular access point for Internet services in the developed world, and it is very likely to become the access device of choice for the huge potential number of users in emerging markets. Human rights issues arising online could migrate to the mobile sector, which already sees its own specific issues. For example, in September 2010, during the outbreak of riots related to rising costs of food, cell phone users in Mozambique found they couldn't send text

7. [http://www.globalnetworkinitiative.org/issues/Manufacturing\\_and\\_Software.php](http://www.globalnetworkinitiative.org/issues/Manufacturing_and_Software.php).

8. See, e.g., <http://news.bbc.co.uk/2/hi/technology/8124735.stm>.

9. [http://www.usatoday.com/tech/news/2009-07-02-china-pc\\_N.htm](http://www.usatoday.com/tech/news/2009-07-02-china-pc_N.htm).

10. <http://www.bbc.co.uk/news/world-asia-pacific-10968906>.

messages.<sup>11</sup> And in October 2010, the Egyptian government imposed a license requirement for sending out bulk text messages.<sup>12</sup>

- As covered by many news organizations around the world, in August 2010, the governments of the United Arab Emirates,<sup>13</sup> Saudi Arabia<sup>14</sup> and India<sup>15</sup> raised concerns that a handheld device could send and receive encrypted messages that governments would be unable to access.<sup>16</sup> Although the device manufacturer and communications service provider ultimately avoided being banned,<sup>17</sup> its predicament is cautionary.
- Government blocking and content policies now also impact the domain registration and Internet addressing system. Web hosting companies have found domains they manage have been blocked, or have found that governments block citizens

**“The jailing of Chinese journalist Shi Tao set off alarm bells for reporters worldwide. It prompted the Committee to Protect Journalists to engage with ICT companies to help ensure that the Internet is open and safe for journalists. The Global Network Initiative is an important first step towards that goal. Journalism is increasingly moving onto the Internet, but that platform is vulnerable to filtering and censorship. If there’s one statistic that sums up why it’s important for us to work with GNI it’s this: more than half the journalists in jail around the world today worked online.”**

— Robert Mahoney, Deputy Director,  
Committee to Protect Journalists

from accessing their services to register certain domains. The “country-code” domains controlled by governments (or in non-English languages associated with certain countries) may require contractual agreements to censor content as a condition of registering web addresses in those domains.<sup>18</sup> Similar requirements may apply to other, new domains.<sup>19</sup> And domain registries are confronting difficult questions regarding requirements that they collect – and forward to the government – detailed personal information from customers who register addresses.

- Various law enforcement and national security agencies are exploring proposals to extend wire-tapping onto the Internet.<sup>20</sup> Extensive media attention has focused on the pros and cons of making Internet communications services subject to the “lawful intercept” requirements that apply to telecommunications, including the risks to national security, the potential that such intercept capabilities could be exploited by hackers, and the inevitability of these issues arising as more and more of our data flows online.<sup>21</sup>

GNI’s response to these challenges looks first to internationally recognised human rights standards, including the United Nations Universal Declaration of Human Rights,<sup>22</sup> The International Covenant on Civil and Political Rights<sup>23</sup> and The International Covenant on Economic, Social and Cultural Rights.<sup>24</sup> These standards represent a broad consensus among governments and societies about (a) the fundamental role of human rights in a global environment, (b) how to integrate free expression and privacy with other rights, such as security, liberty and economic rights, and (c) the framework for ongoing discussion and dialogue.

11. See, e.g., <http://allafrica.com/stories/201009230933.html>;
12. <http://www.google.com/hostednews/afp/article/ALeqM5grcsHilvOKbNXy9pEys0vHOS8Wg>.
13. <http://english.aljazeera.net/news/middleeast/2010/10/20101013161343686704.html>.
14. <http://www.arabtimesonline.com/NewsDetails/tabid/96/smld/414/ArticleID/157781/t/uae-ban-on-blackberry-a-security-%e2%80%98badge-of-honor%E2%80%99/Default.aspx>.
15. <http://english.aljazeera.net/news/middleeast/2010/08/2010844243386999.html>.
16. <http://indiatoday.intoday.in/site/Story/109680/the-blackberry-storm.html?page=0>.
17. <http://www.telegraph.co.uk/technology/blackberry/7922936/Future-is-no-longer-so-sweet-for-BlackBerry.html>.
18. See, e.g., <http://www.telegraph.co.uk/technology/blackberry/8050443/BlackBerry-escapes-UAE-ban.html>.
19. See, e.g., <http://www1.cnnic.cn/html/Dir/2005/03/24/2861.htm>, Article 27.
20. <http://arstechnica.com/old/content/2007/02/8928.ars>.
21. <http://www.nytimes.com/2010/09/27/us/27wiretap.html?ref=us&pagewanted=all>.
22. <http://arstechnica.com/tech-policy/news/2008/04/fbi-wants-to-move-hunt-for-criminals-into-internet-backbone.ars>.
23. <http://www.un.org/Overview/rights.html>.
24. <http://www2.ohchr.org/english/law/ccpr.htm>.

**“Governments no longer accept the Internet and its applications as they are found – they now aspire to reshape these technologies. GNI has formed at a crucial time, helping to sort out legitimate requests and demands from overreaching ones, ensuring that the desires of regulators are weighed within a larger context valuing innovation, freedom, and protection from abuse.”**

**– Jonathan Zittrain, Professor of Law, Harvard Law School; Co-Fonder and Co-Faculty Director, Berkman Center for Internet & Society**

Taking this framework of internationally recognized human rights as a starting point, GNI focuses on providing good practice guidance for ICT companies. This guidance is developed with an understanding, however, that everyone – Internet users, ICT companies and their employees, academics, activists, business interests, policymakers and policy implementers – has a vital role in reducing human rights risks and promoting an Internet that is safe, thriving, and protective of free expression and privacy.

Internet users can promote good governance on these issues by (a) making known their views, both to governments and to service providers; (b) learning to identify and mitigate safety and privacy risks online; and (c) calling for greater transparency from companies and governments.

Similarly, governments have, not only the primary obligation to uphold human rights, but also an important role to play in the way in which they interact with the ICT industry and civil society to

implement law and policy. Governments should, within their domestic spheres, protect national security and enforce laws without impinging unduly on human rights while respecting and upholding free expression and privacy. As international actors, governments must demonstrate leadership in forging greater international consensus. The international community needs to agree on balanced and predictable rules relating to government access to data, including assertions of jurisdiction over data by law enforcement and other government agencies. Government support for international efforts to promote and protect free expression and privacy is also critical.

GNI's development of good practice is strengthened by the diversity of its participants and the different perspectives they bring. Civil society and business interests may sometimes appear disconnected from one another or at odds on these issues – and in some cases these divisions are real. But the participants in GNI have come together in a multi-stakeholder process, so that each can contribute to the development of practical solutions.

GNI is uniquely positioned to facilitate this dialogue and thereby provide guidance to ICT companies striving to uphold human rights and avoid complicity in human rights violations. GNI member companies can leverage the on-the-ground expertise of civil society organization members, the detailed analysis and considered judgment of academic members, and the support and influence of investors to develop considered responses to the requests and demands they face from governments around the world. In so doing, participating companies can better respond to the concerns of users and the broader public.

# GNI: GOVERNANCE AND WORK

GNI's Governance Charter<sup>25</sup> establishes GNI's approach to governance and its primary organizational elements. The Governance Charter describes how the governance structure will ensure integrity, accountability, relevance, effectiveness, sustainability and impact.

GNI was formally incorporated in the United States on 26 February 2010. Its first Executive Director, Susan Morgan, began work on 1 June.

GNI is completing recruitment of an Independent Chair to provide objective, innovative leadership. GNI's Board of Directors functions to further the Principles and to ensure that the organization's work fulfils GNI's vision. The Board currently has eleven members (five seats remain open for future member companies). The current composition of GNI's Board is as follows:

## ICT Companies

Chuck Cosson, *Microsoft*

Ebele Okobi-Harris, *Yahoo!*

Lewis Segall, *Google*

## Civil Society Organizations

Arvind Ganesan, *Human Rights Watch*

Leslie Harris, *Center for Democracy & Technology*

Robert Mahoney, *Committee to Protect Journalists*

Meg Roggensack, *Human Rights First*

## Investors

Bennett Freeman, *Calvert Group*  
(Secretary of the GNI Board)

Adam Kanzer, *Domini Social Investments LLC*

## Academics and Academic Organizations

Colin Maclay, *Berkman Center for Internet & Society at Harvard University*

Rebecca MacKinnon, *New America Foundation*  
(personal capacity)

The Board has constituted the following committees to carry out its work: (a) Audit, (b) Executive and Management, (c) Governance and Accountability, (d) Outreach and Communications, and (e) Policy and Learning.

GNI's work arises in the context of governments asking ICT companies to take actions that may impair the free expression and privacy rights of users. GNI works in the following four areas:

1. **Establishing a framework for responsible company decision-making and action:** Our Principles, Implementation Guidelines and Governance, Accountability & Learning Framework take as their starting point universal, internationally-recognized human rights standards. The United Nations "Protect, Respect and Remedy" Framework, presented by the Secretary-General's Special Representative for business and human rights (Harvard professor John Ruggie) and unanimously welcomed by the Human Rights Council in 2008, has also been a prime influence. GNI's Principles, Implementation Guidelines and Governance, Accountability & Learning Framework are designed to help companies:
  - respect and protect the free expression and privacy rights of users when companies respond to government demands, laws and regulations

**"The declaratory era of CSR is over: It's not enough for companies to say that they respect human rights, they must know and show that they are doing so. GNI is an important platform for ICT companies to do just that: to develop robust policies and processes in collaboration with other experts, and share their learnings with the public. This report is an important first step."**

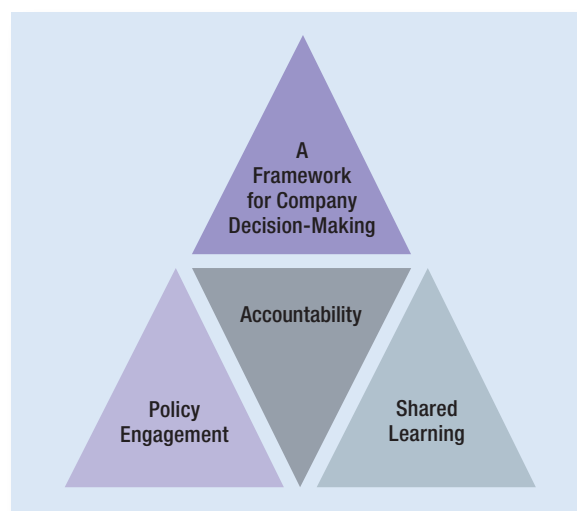
— Professor John Ruggie, UN Secretary-General Special Representative on business and human rights

25. <http://www.globalnetworkinitiative.org/charter/index.php>.

- integrate into their decision-making, policy implementation and organizational cultures responsible policies and procedures that protect and advance free expression and privacy
- communicate policies and practices with users.

Our central vision and purpose are clear. However, the Principles, Implementation Guidelines and Governance, Accountability & Learning Framework are not intended to be static, but rather documents that will be adapted and developed at the Board's direction to keep pace with issues as they emerge, with GNI's anticipated growth, and to reflect the learning and maturity of GNI.

2. **Fostering accountability:** GNI companies commit to an independent assessment process to evaluate their implementation of the Principles. GNI helps to identify issues and work collaboratively to find solutions. The assessment process provides a sense of how the companies are taking responsibility for protecting the freedom of expression and privacy of their users. In so doing, companies also demonstrate the integrity of the GNI process and the trust among constituents and stakeholders, including users, industry participants, civil society organizations, academics, business interests and governments. The first external assessment of GNI member companies will begin in 2011. Details about the process are described on pages 11-12.
3. **Promoting policy engagement:** Because GNI provides a single platform for collaboration between ICT companies, civil society organizations, investors and academics, GNI is uniquely situated to engage governments, intergovernmental organizations and international institutions on issues related to free expression, privacy and ICT company practices. While GNI participants have a long history of policy engagement, more integrated GNI efforts have become possible only with the organization's recent increase in capacity. GNI has already had numerous interactions (both formal and *ad hoc*) with representatives of diverse governmental institutions, and GNI is currently in the process



of creating more structured channels for transparent, regular consultation with governments. Notwithstanding that GNI is at the beginning stages of this work, two public examples of GNI's work in this arena during 2010 include:

- In June 2010, GNI participated in a workshop sponsored by the Organisation for Economic Co-operation and Development (OECD) on intermediary liability.<sup>26</sup> At this workshop, we put forward the view that intermediary liability for ICT companies can ultimately impair free expression and, in some jurisdictions, the potential liabilities can result in companies self-censoring to reduce their financial and legal risks.
- In March 2010, we submitted a written statement to support and assist the U.S. Senate Judiciary sub-committee on Human Rights and the Law in its hearing on "Global Internet Freedom and the Rule of Law, Part II."<sup>27</sup> GNI's statement identified key human rights challenges and opportunities for collaboration to promote Internet freedom.

These contributions to policy dialogue are merely a beginning. GNI is committed to continuing and expanding its policy engagement with governments, intergovernmental organizations and international institutions on issues relevant to its work.

26. [www.oecd.org/dataoecd/42/52/45509346.pdf](http://www.oecd.org/dataoecd/42/52/45509346.pdf).

27. [http://www.globalnetworkinitiative.org/newsandevents/GNI\\_Hearing\\_Statement\\_20100302.php](http://www.globalnetworkinitiative.org/newsandevents/GNI_Hearing_Statement_20100302.php).

**“As ICTs become increasingly integral to people’s lives and livelihoods, government strategies for control have adapted as well, in pervasiveness, sophistication and reach. This evolving landscape constantly raises new and challenging questions for a broad range of ICT companies and other stakeholders. A collaborative and adaptive model such as GNI is well positioned to formulate principled responses and guidance for both companies and policy-makers alike – leveraging data, experience, and empirical research – to better understand threats, trends and the impact of interventions.”**

— John Palfrey, Faculty Co-Director, Berkman Center for Internet & Society Henry N. Ess Professor of Law and Vice Dean for Library and Information Resources at Harvard Law School

4. **Enabling shared learning:** A central aspect of our work is fostering collective learning among GNI participants. While this learning can take a variety of forms – including informal exchanges, Board interactions, one-on-one conversations and committee calls – collaboration and shared learning on ICT issues are fundamental to the sustainability and impact of the GNI model.

Among GNI’s core membership benefits is the trusted interaction that participants enjoy. GNI offers member companies the confidential setting and relationships to explore challenges and exchange information on how to approach and resolve ICT issues with human rights groups, academics and investors, and vice versa (often as events are unfolding).

In addition to GNI’s internal learning opportunities, we have also created forums for members and non-members to learn with and from each other about emerging ICT issues, including participation in our “live issue” conference calls. For example, current activities include:

- We host a series of calls about account deactivation and content removal. The calls have examined a range of resolutions to various ICT issues and involved participation from activists. We are also compiling a wiki to present the relevant policies, documents and best practices distilled from these calls.
- We also host a series of calls on the issues of intermediary liability and export controls, exploring different international legislative and regulatory regimes, seeking to integrate diverse perspectives, concerns and practices. As with the issue of account deactivation and content removal, we are compiling a wiki of the insights derived from the call and associated resources.

In the coming year, GNI will continue this productive approach to addressing new ICT issues as they arise. In addition, GNI will explore other forms of interaction to best advance our collective understanding.

Since launching, GNI has continued an active dialogue with diverse companies, in order to encourage their membership or, alternatively, to understand barriers to their active participation. In February 2010, we held an implementation dialogue to explore whether there was a current need to adapt the Principles.<sup>28</sup> This dialogue clarified that, while the Principles apply across the sector, four areas present opportunities for potential development:

1. free expression and privacy risks associated with product functionality, as opposed to content
2. conducting human rights due diligence before entering into relationships with potential partners and customers, as well as understanding the intended use of products, services or functionalities
3. free expression and privacy concerns implicit in consulting services provided alongside the product, service or technology
4. responding to government demands and mandated standards, while simultaneously acting responsibly to protect human rights.

Further dialogue in the autumn of 2010 has helped us design a programme of work for 2011 to address the issues raised. Our focus will depend, in part, on the companies that express interest in working with us.

28. [http://www.globalnetworkinitiative.org/cms/uploads/1/GNI\\_Written\\_Statement\\_2010\\_03\\_01\\_1.pdf](http://www.globalnetworkinitiative.org/cms/uploads/1/GNI_Written_Statement_2010_03_01_1.pdf).

# GNI: CREATING ACCOUNTABILITY AND TRANSPARENCY

The independent assessment to which GNI member companies commit has the following benefits:

- It promotes respect for and protection of the free expression and privacy rights of ICT users by ensuring that companies are implementing the Principles effectively.
- It provides a competitive advantage to GNI member companies by demonstrating that they are living up to their commitments and earning the trust of stakeholders such as users, investors and civil society organizations.
- GNI member companies share an external, independently assessed commitment (made by a group of companies, including competitors) to respond to government demands in a manner that respects human rights. Member companies enjoy the strength of speaking with a united voice.
- The independent assessment process provides a genuine opportunity for companies to build their capacities, through constructive, confidential feedback.
- Assessment informs the ongoing process of refining GNI's Principles, Implementation Guidelines and Governance, Accountability & Learning Framework. Without assessment, GNI would lack ready means for knowing whether the Principles are effective in reducing human rights risks to users, or how to calibrate the Principles to

enhance their effectiveness. Assessment thereby strengthens GNI's integrity, and all members – as well as users – benefit.

Whatever their size or market reach, committing to independent assessment is a significant step for GNI member companies. For this reason, companies have two years from the date they join GNI to build the capacity to make the Principles and Guidelines operational in ways appropriate to their businesses, including establishing processes to evaluate what risks to free expression and privacy are relevant to their operations. This period is an opportunity to learn from other members about the assessment process, and to seek guidance and advice from other constituencies about implementation of the GNI Principles.

GNI provides both a common baseline for implementation of the Principles, as well as flexibility. Implementation may vary across different types, sizes and structures of companies, and across different lines of business. Some GNI guidelines will apply in every case: for example, GNI member companies must have channels for regular communication at a senior level about risks to human rights identified in the company's operations, as well as a person or team within the company with responsibility for implementing GNI's Principles. That established, however, given the many different companies in the sector, spanning different business models, products, services, technologies and markets of operation, the way in which companies implement the Principles will be tailored to their own

**“The Global Network Initiative recognizes that companies face daily pressures to limit services in ways that affect the free expression and privacy rights of their users. As Human Rights First knows firsthand from working with frontline activists, when companies ‘go it alone’ in complying with government demands, they put the rights of users at risk. GNI was established to help companies make decisions which preserve and promote an open and accessible information infrastructure, and to ensure that they are accountable to the public for the decisions they make. We’re committed to ensuring that the GNI’s approach becomes the global standard by which ICT companies are judged.”**

– Meg Roggensack, Senior Advisor for Business and Human Rights, Human Rights First

**“GNI is a vitally important initiative to protect freedom of expression and the right to privacy on the Internet as so many companies in the ICT sector operate across a range of countries – from authoritarian to democratic – whose governments deliberately or inadvertently threaten those rights. It is essential that the GNI principles are implemented by a widening circle of companies across the sector in ways that are transparent and accountable. This first public report is a step towards achieving such transparency and accountability in the interests of Internet users, ordinary citizens and investors as well as the companies themselves.”**

– Bennett Freeman, Senior Vice President for Social Research and Policy, Calvert Group

contexts and characteristics. Such adaptations will affect the assessments; indeed, a critical step in the assessment process is articulating why, and gaining feedback about how, the company’s chosen method of implementation works for its business model and circumstances.

The upcoming assessment of current GNI member companies’ implementation of the Principles will take place over 2011-2012: (a) in 2011, the assessment will focus on the processes, systems and training that the company has established to ensure compliance with the GNI Principles; and (b) in 2012, the assessment will examine specific company responses to government demands implicating free expression and privacy, and seek to learn from those experiences. The goal of examining specific responses is not to audit whether the company made the “right” choice in a given experience, but to assess whether the processes and systems established earlier work in the context of actual practice. Here is a brief overview:

## 2011 Assessment

1. Using criteria established by GNI to determine assessor eligibility, the company appoints its assessors. An independent assessor could be an individual or, more likely, a team. Qualified assessors may have varying types of expertise: law, accounting or business consultants may all qualify, as long as the assessor is independent of the company and substantively qualified to perform the task (both determined by GNI criteria)
2. To initiate the assessment, the company prepares a report, using guidance that GNI has developed to describe the company’s processes for implementing the Principles. In accordance with confidentiality agreements governing the assessment process, the independent assessor alone has access to this report

3. The independent assessor reviews the report, and is also likely to interview relevant personnel to get a clear sense of the company and its processes to ensure they are fit for purpose for implementing GNI’s Principles
4. The independent assessor reviews relevant company documentation and data, with exceptions for instances where providing such access would either (a) be prohibited by law, or (b) jeopardize trade secrets or attorney-client privilege; in which case the company may withhold such information (recognizing the potential implications for the ability to conduct a full assessment)
5. The independent assessor produces a written evaluation of the company’s approach to implementing the GNI Principles, which is shared with the company and GNI staff
6. The GNI Executive Director prepares a report to the Board and to the public, incorporating the findings of the assessment.

## 2012 Assessment

1. The Board of GNI accredits a number of independent assessors, building on the experience gained in 2011 in terms of available and capable candidates
2. The member company selects its independent assessor from the pool of accredited assessors
3. The member company prepares a report, using guidance developed by GNI, to describe the company’s processes for implementing the GNI Principles, and also specific examples of application of the Principles to actual experience. Again, confidentiality agreements govern this report, so that only the independent assessor may review it



4. The independent assessor conducts the assessment, reviewing the report, company documentation and data and conducting interviews with relevant employees
5. The independent assessor reviews relevant company documentation and data, with exceptions for instances where providing such access would either (a) be prohibited by law, or (b) jeopardize trade secrets or attorney-client privilege; in which case the company may withhold such information (recognizing the potential implications for the ability to conduct a full assessment)
6. The independent assessor prepares a report evaluating the response of the company to specific government demands, including a judgment of the effectiveness of the company's implementation of the GNI Principles in its response(s)
7. Where warranted, the independent assessor recommends options for better implementation of the GNI Principles
8. The member company may review and respond in writing both to draft and final reports of the independent assessor. These responses will be provided to GNI staff for review and evaluation
9. GNI staff present the outcome of the assessment to the Board
10. The GNI Board will determine whether the company is compliant with the GNI Principles. The Board's decision will be included in GNI's annual report to the public
11. GNI member companies report on their progress in implementing the GNI Principles through their own communications to the public.

Assessments are annual once a company reaches its third year of membership in GNI.

GNI will report publicly on its work and progress.

# GNI: DRIVING CHANGE

**G**NI's unique strength is its breadth and diversity of membership: before GNI formed, many of our core members were either unknown to or critical of one another. But a shared commitment to creating and, subsequently, promoting the GNI Principles, along with a belief in the effectiveness of the multi-stakeholder process, has allowed these differing organisations to collaborate and contribute, as individual entities and jointly, to pioneer practical solutions to ICT issues.

Each constituency within GNI plays a role in driving change, both with respect to helping companies make the right decisions in tough situations, and to supporting a shared mission to improve respect for freedom of expression and privacy through the advancement of the Principles. While these objectives are collectively held, each participant may play a different type of role in GNI, depending on the type of organization:

- **ICT companies** commit to upholding the GNI Principles by implementing them within their organizations, by undertaking independent assessment to evaluate the effectiveness of their implementation, and by publicly reporting on their progress. The work of these company members is especially critical in light of the worldwide economic power they represent: the revenue of GNI's current company members, Google, Microsoft and Yahoo!, exceeds that of some nations, and their reach spans the globe. Their willingness to commit to high standards in their operations sets a leadership bar and, at the same time, the diversity of their operations illustrates that implementing GNI's Principles is an achievable goal for ICT companies. Greater detail about the work of GNI's member companies follows on pages 15-22.
- **Civil society organizations**, including human rights and press freedom groups, participate in GNI because they recognize that the ICT sector must respond to government demands to comply with laws and policies that implicate free expression and privacy. GNI's Principles require member companies to respond to these demands in ways that preserve and promote free expression and privacy. Civil society members support member

**“GNI has taken on a hugely important and dynamic suite of issues, employing a blend of familiar and novel approaches to create a robust, collaborative platform for learning and action that is designed to evolve alongside – and hopefully, ahead of – the complex challenges faced by both its members and societies around the world.”**

– Colin Maclay, Managing Director, Berkman Center for Internet & Society at Harvard University

companies through their in-depth knowledge and expertise on human rights issues and their direct connection to people on the ground. Civil society members also contribute to GNI's responses to the challenges of upholding human rights in the ICT environment and ensure that GNI addresses credibly and transparently the concerns of users most directly affected.

- **Investors** have a particular interest in encouraging ICT sector companies to respect the rights of their users and protect their brands, while continuing to operate in diverse and challenging countries and markets around the world. Investors therefore have been committed to building GNI because they recognize that censorship and surveillance pose direct threats to the long-term viability of ICT sector companies, as well as to users of these technologies around the world. Investors commit to the GNI Principles by discussing GNI and its benefits with the companies in which they invest, by incorporating these issues into their investment decision-making, and by seeking to influence companies to join GNI and to otherwise address the issues implicating human rights in the ICT environment through shareholder resolutions, proxy voting and company communications.
- **Academics and academic organizations** have contributed a wide array of research findings and analysis that have enhanced our understanding of, and approaches to, the human rights issues arising within the ICT landscape. Academics have worked with GNI members and affiliates to bring diverse perspectives and deeper analysis to the discussions surrounding the Green Dam Youth

**“Governments are increasingly pressing the ICT sector to implement policies that impact the free expression and privacy rights of users. For tech companies who want to do good and do well, the GNI provides a forum for charting an accountable and ethical path forward. GNI aims to articulate a global standard of care, while providing practical guidance for companies facing complex real-time challenges.”**

— Leslie Harris, President & CEO, Center for Democracy & Technology

Escort software, account deactivation, intermediary censorship, and other emerging issues. Academics have led our development of online and wiki-based resources. Their practical and empirical research on government controls and the rise of online filtering, censorship and surveillance has informed company best practices and identified relevant trends.

Since the launch of GNI, these groups collectively have driven change in three primary ways:

1. Promoting the Principles, the Implementation Guidelines and the Governance, Accountability & Learning Framework in their work and their conversations with others in the business, human rights, academic, journalist, CSR and investor communities
2. Creating platforms for, participating in, and otherwise contributing to, public dialogue about these issues and additional learning within GNI
3. Preparing to implement, or supporting the work of GNI member companies as they implement, GNI's Principles.

In this first annual report to the public, the work of GNI member companies merit special focus.

The following is a detailed description and status report on the progress that our current three company members (Google, Microsoft and Yahoo!) have made implementing the Principles. While they have yet to undergo their first assessments, the breadth of their experiences illustrates how companies are tailoring implementation to meet the specifics of their company profiles.

These descriptions are provided by the companies themselves to illuminate three points:

- i. how GNI member companies are implementing the Principles
- ii. how GNI member companies operate differently because of their membership
- iii. how GNI membership has helped address a problem or problems.

**“The ICT sector is designed to further freedom of expression and depends upon strong privacy protections to maintain consumer trust and confidence. There is a business imperative, therefore, to defend these fundamental human rights.”**

— Adam Kanzer, Managing Director & General Counsel, Domini Social Investments LLC

## Google

Google's mission is to organize the world's information and make it universally accessible and useful. Since the company's inception, free expression has been one of Google's core values, as has been protection of user privacy. Google's Code of Conduct requires respect for the privacy of users' information and implementation of the internationally recognized human rights of free expression and privacy in the context of government demands for information. Revenue last financial year was \$23.65 billion. Google has over 20,000 employees and locations in over 35 countries. Its products are split into the following categories: (a) search, (b) advertising, (c) applications, and (d) mobile.

A committee composed of senior representatives from its legal, ethics and compliance, policy and communications, product, and engineering teams oversees implementation of GNI's Principles. This committee meets quarterly and reports to the senior legal executive officer, who reports directly to Google's CEO.

Google's implementation of GNI's Principles relies on corporate infrastructure to ensure that human rights concerns are mainstreamed into Google's business operations. To this end, Google has established protocols for ensuring consideration of free expression and privacy rights in the following contexts:

- When responding to a government request for user information, for removal of content, or to restrictions on the provision of information, Google undertakes a legal examination to determine the validity of the request or restriction in light of applicable law
  - Google's policy requires that Google receive a government request via valid legal process before Google will disclose non-public user data, with the following exceptions: (1) an emergency where disclosure is needed to avert
- When deciding to enter a particular market, whether by opening an office or establishing a data center, Google analyzes the political, legal and cultural conditions. If warranted by the risks to user privacy or free expression that it identifies in a particular jurisdiction, Google may limit its delivery of certain products or services, offer them from outside the jurisdiction and/or store sensitive user data elsewhere
- When developing and launching products, Google conducts a legal review to identify free expression and privacy issues, as well as to propose methods for minimizing these risks. Products, services or technologies that collect personally-identifiable information or involve user-generated content are especially likely to implicate these concerns and therefore warrant close review. Last February, for example, Google introduced Buzz, a social networking application. Immediately after launch, Google made significant product improvements to respond to concerns about privacy.<sup>30</sup>

imminent loss of life or serious injury; (2) the user has consented to the disclosure, or (3) disclosure is necessary to defend Google rights and property. When requests from government officials appear overbroad, Google negotiates with the aim of limiting the scope of the request

- Google strongly defends the rights of its users to think, speak and share ideas and thoughts. Google seeks to make available the maximum content permissible by law. In cases requiring removal of content, Google strives to implement removal orders as narrowly as possible (e.g., removing content within a particular country domain rather than a global domain). Whenever Google removes content, it informs the user and, in most instances, forwards the removal request to Chilling Effects.<sup>29</sup>

**“In a time of rapid change and increasing challenges to the free flow of information on the Internet, GNI has proved remarkably valuable to Google. The ties that we have established to the NGO community — through the formal guidelines and informal work — have helped warn us of upcoming dangers, protect the rights of our users and promote online free expression in the U.S., Europe and beyond.”**

— Lewis Segall, Senior Counsel, Global Ethics and Compliance at Google

29. <http://www.chillingeffects.org/>.

30. See <http://gmailblog.blogspot.com/2010/02/new-buzz-start-up-experience-based-on.html>.



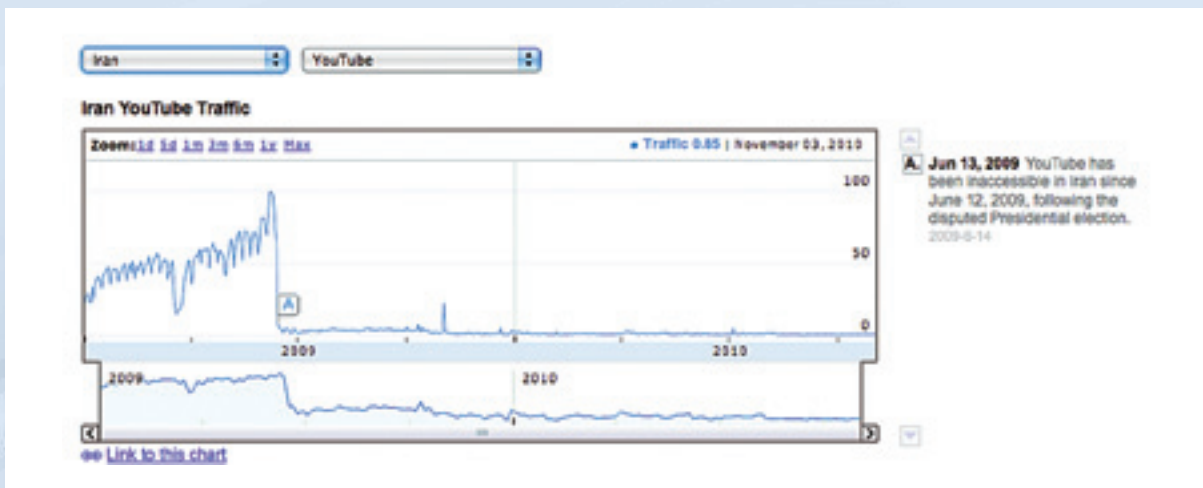
Screen shot of Google’s Transparency Report, which tracks government requests to limit access to information or seek information about individual Internet users.

Google also implements the Principles through support of and engagement with individuals, organizations and entities that further the cause of user freedom of expression and privacy. Google’s support includes the following:

- Google provided assistance to NGOs that support free expression in the form of financial aid, in-kind advertisement space and technological capacity building. The purpose of Google’s assistance is to

raise awareness about human rights risks in the Web 2.0 and ICT environment; to train activists, bloggers and traditional journalists; and to grow these NGOs

- Google sponsored or supported awards for global Internet activities like the Reporters Without Borders “Netizen” prize<sup>31</sup> and the Global Voices “Breaking Borders” award<sup>32</sup>
- With the Central European University, Google sponsored the “Internet at Liberty 2010” conference, which brought together more than 300 participants from 74 countries<sup>33</sup>
- In both Europe and the U.S., Google engaged with governments on policy development:
  - Google contributed to the initiative on Internet freedom propounded by the French and Dutch governments, as well as to the Swedish government’s work on a report for the U.N. Special Rapporteur on Freedom of Expression
  - In the aftermath of U.S. Secretary of State Hillary Clinton’s speech on global Internet freedom, Google engaged with Executive and Congressional leaders and staff on the issues she raised



Screen shot of Google’s Transparency Report, which tracks global availability of Google services.

31. <http://en.rsf.org/iranian-women-s-rights-activists-12-03-2010,36718>.  
 32. <http://globalvoicesonline.org/2010/05/07/announcing-the-winners-of-the-breaking-borders-award/>.  
 33. <https://sites.google.com/a/pressatgoogle.com/internet-at-liberty-2010/>.

- In collaboration with other industry associations, Google is assisting in building the case that blocking the free flow of information is a barrier to trade
- Google additionally is a leader in the Digital Due Process coalition, which advocates updating U.S. surveillance law.<sup>34</sup>

Two examples from the past year illustrate how Google implements the GNI Principles to further user privacy and freedom of expression:

1. Like many companies, Google regularly receives requests from governments for the removal of content from its services or for information about its users. The company also occasionally finds its services blocked or filtered around the world. To promote transparency around these issues, the company built an online Transparency Report<sup>35</sup> as a deterrent to censorship and to educate users and others. The Transparency Report not only provides details about government requests for content removal (including information on the number of removal requests received and the number complied with) and user data, but it also contains a traffic tracking tool to provide nearly real-time information about disruptions to Google services around the world. Each traffic graph shows historic traffic patterns for a given country and service and indicates whether a disruption is government-induced. By showing outages, the traffic graphs visually depict disruptions in the free flow of information, whether due to a government blocking information or a cable being cut.
2. In December 2009, Google discovered that it and more than 20 major companies had been the target of an unusually sophisticated attack, and

that a primary goal of the attackers was accessing the Gmail accounts of Chinese human rights activists. Separate from these attacks, Google discovered that the Gmail accounts of dozens of human rights activists interested in China were routinely accessed using phishing scams and malware, not via Google.

These events – combined with Chinese attempts over the previous year to further limit free speech on the web – led the company to stop censoring search services – Google Search, Google News and Google Images – on Google.cn. Starting in March 2010, users visiting Google.cn were redirected to Google.com.hk, where they were offered uncensored search in simplified Chinese.

In June 2010, conversations with Chinese government officials clarified that if the company continued redirecting users automatically, its Internet Content Provider license would not be renewed. Without an ICP license, Google wouldn't be able to operate a commercial website like Google.cn. Many Chinese users were vocal about their desire to keep Google.cn alive.

After looking at alternatives, Google decided to take users to a landing page on Google.cn that linked to Google.com.hk – where users could conduct uncensored web search or continue to use Google.cn services like music and text translate. This approach ensured that Google stayed true to its commitment not to censor results on Google.cn and to give users access to Google's services from one page.

In July 2010, the Chinese government renewed Google's ICP license.

34. <http://www.digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163>.

35. <http://www.google.com/transparencyreport>.



## Microsoft

Microsoft is a large multinational company with annual revenue of \$62.5 billion reported for the fiscal year ended June 30, 2010, almost 90,000 employees and 700,000 partners in over 100 countries. There are five major business segments: (a) Windows and Windows Live, (b) Server and Tools Business, (c) Online Services Division, (d) Microsoft Business Division, and (e) Entertainment and Devices Division.

Oversight of Microsoft's implementation of the GNI Principles and Guidelines is carried out by an Executive Board comprised of the General Counsel and Chief Research and Strategy Officer. Two Corporate Vice Presidents, as delegates of the Executive Board, have daily oversight and responsibility for the Freedom of Expression and Privacy Working Group. This group constitutes the senior human rights team referred to in the GNI Guidelines. The two Vice Presidents and the working group review GNI issues quarterly, while the working group meets on a more frequent basis. Microsoft keeps its Board of Directors apprised of its implementation efforts and related material issues by including information on free expression, privacy and other issues of GNI concern in quarterly reports to its Board of Directors. Privacy and free expression issues have also been incorporated in its enterprise risk management processes.

Taking a materiality approach to GNI Implementation, Microsoft has sought to identify markets where fundamental rights are likely to be most at risk. Microsoft uses the annual work from Freedom House, which, in 2010, designated more than 50 countries as Not Free.<sup>36</sup> Microsoft treats these countries as High Risk Markets. In addition, Microsoft identifies High Risk Services by considering a variety of factors, including the number of users, historical data on the number of demands from government authorities, and whether it is a general communications service likely to be used for free expression. Of its services,

Bing presents the greatest potential for restriction of content due to government demands while Windows Live Hotmail and Windows Live Messenger present the greatest potential of generating interest from government authorities for user information.

Microsoft had existing policies and procedures for responding to government requests for user data or to filter or remove content. As part of its implementation of GNI's Principles, Microsoft supplemented these with a corporate Freedom of Expression policy, which applies across all Microsoft's online and communication services.

In particular, Microsoft's Freedom of Expression policy builds on GNI's foundation in international human rights laws and standards to draw distinctions between content which:

- is protected under international standards of free expression: Microsoft will not filter or remove such content without a legally binding notice, and Microsoft will take steps to minimize the impact of such demands
- is illegal in a particular geography and which international standards accept as reasonably restricted (e.g., explicit adult content): Microsoft may take voluntary steps to address government requests about such content
- Microsoft determines violates its terms of use or other agreements with end users: Microsoft will make discretionary business decisions in these situations. Users are presented with the terms governing their use of Microsoft services.

For Bing, features have been incorporated into the product design of the service to minimize the impact of government demands by enabling restrictions of content only for users in the market issuing the restriction and who use the version of Bing tailored to that market. Bing also provides notice to users

**“Microsoft’s mission is to enable people and organizations to realize their full potential, including the social and economic opportunity that technology can unlock through access to information. GNI helps us further that mission by creating a systemic approach to respecting user rights and a forum for ongoing learning on free expression and privacy.”**

**—Chuck Cosson, Senior Policy Counsel at Microsoft**

36. <http://www.freedomhouse.org/template.cfm?page=363&year=2009>.

directly on the page displayed following a query for which results have been restricted which explains that some results have been removed due to a government demand.

When considering hosting user data in a new location, Microsoft's existing data geo-location policy addresses the GNI guideline that companies will assess the human rights risks associated with the collection, storage and retention of personal information in the jurisdictions where they operate. This policy stipulates that legal obligations and human rights risks are analysed before hosting, in a new market, the types of user data of greatest interest to governments and which would most impact users' rights should such data be used in a manner inconsistent with international standards on privacy and freedom of expression. Reports from third party organizations such as Freedom House and The World Bank Institute are consulted as a part of this process. Senior executive approval is required before data can be located in a new market.

Microsoft will require all third parties who collect, handle or use personal information to comply with Microsoft's policies and practices relating to maintaining confidentiality, and has an established Vendor Privacy Assurance Program (VPA) to help ensure compliance with this requirement. This is an additional example of how existing processes were incorporated into a GNI implementation program.

In addition to the requirements in Microsoft's VPA, in High Risk Markets, Microsoft will add a human rights risk assessment to the due diligence process for certain arrangements with third parties that involve High Risk services. Senior executives will review the results of the risk assessment and any proposed risk mitigation measures to determine whether it is appropriate for Microsoft to proceed.

Microsoft's engagement in public policy around issues relating to freedom of expression and privacy is extensive, including in part:

- Calling for industry and governments worldwide take action to strengthen privacy and security in cloud computing
- Working with the Council of Europe Project on Cybercrime

- Convening the U.S.-China Internet Industry Forum
- Participating in discussions of network-based filtering process in Australia, Hong Kong, and Europe
- Working to explore the contours of free expression in relation to rights to human dignity, and to respond to concerns about cyber-bullying.

Given the profile of its business, Microsoft's work on public policy naturally extends beyond regulation of online services to matters of intellectual property protection. The value of multi-stakeholder collaboration on these issues was brought home strongly this year when *The New York Times* documented a challenge Microsoft faced in Russia regarding property rights enforcement actions against the media, NGOs, and others engaged in public advocacy. As *The New York Times* reported, NGOs had for some time believed that the purpose of such enforcement actions was harassment and the restriction of free expression.<sup>37</sup>

Microsoft staff had already been looking at these issues, and they listened to human rights advocates in determining how to best respond. Microsoft welcomed the human rights groups' recommendations, and has been able to draw on their expertise as it works to address them. For example, one way Microsoft responded to this situation in Russia was by creating a one-time unilateral license for the software already on the computers of eligible NGOs and small media organizations in certain markets. Input from human rights groups helped inform Microsoft's choice of markets and the scope of the license.

Microsoft identified at least two inter-related challenges as it has worked to implement the GNI Principles and Guidelines. The first is jurisdictional, as it isn't clear in international law which government entities can assert jurisdiction over online service providers. Microsoft's position is that the location of user data is the key determinant of whether a government may compel disclosure. Many governments around the world demand disclosure of data based on other factors, such as the use of a foreign service by local citizens. Additionally, U.S. courts hold that a company with a presence in the U.S. is obligated

37. [http://www.nytimes.com/2010/09/12/world/europe/12raids.html?\\_r=1](http://www.nytimes.com/2010/09/12/world/europe/12raids.html?_r=1).



to respond to a valid demand for information from the U.S. government regardless of the location of that information. This creates challenges in assessing privacy risks by focusing solely on data location.

The second challenge is the complexity this jurisdictional ambiguity creates for communicating clearly and transparently with users about their rights and,

in particular, which generally applicable laws and policies require Microsoft to provide personal information to government authorities. This is particularly difficult to do with certainty when operating in multiple markets, where user data may be stored in various locations, and where the location of the user may not remain constant.

## Yahoo!

Yahoo! was founded on the principle that promoting access to information improves people's lives and enhances their relationship with the surrounding world. Yahoo!'s revenue exceeds \$6 billion. It employs approximately 14,000 people, and provides services in more than 50 countries.

Yahoo! has formally established a dedicated Business & Human Rights Program (BHRP) in order to lead its efforts to make responsible decisions in the areas of free expression and privacy. The BHRP is situated within Yahoo!'s legal team to provide a central vantage point for reviewing and advising on business decisions that might implicate human rights.

A full-time core team, including senior level employees, guides, directs and manages the BHRP. This team is also responsible for the implementation of GNI's Principles, Guidelines and Governance, Accountability & Learning Framework. To support the work of the BHRP, Yahoo! has additionally established a virtual team comprised of senior level employees, including representatives from Yahoo!'s product, law enforcement, security, public affairs, investor relations and global policy divisions. The virtual team's membership includes geographic representation from the United States, Asia, Europe, Latin America and the Middle East. This virtual team ensures that Yahoo!'s implementation of GNI's Principles is connected to business strategy, and it disseminates policies and procedures created by the BHRP.

The BHRP's work focuses on (a) responsible company decision making, (b) free expression and privacy, (c) multi-stakeholder collaboration and engagement.

Responsible internal company decision-making is central to the BHRP's mission.

- The BHRP team conducts employee training and in-depth reviews with employees and teams who have responsibility for content moderation and/or who have access to user data in the performance of their duties at Yahoo!. The trainings provide employees with a background on the legal and moral foundations of the company's human rights obligations, the relevant GNI Principles, Implementation Guidelines and Governance, Accountability & Learning Framework provisions, and specific guidance on relevant processes and procedures. To date, the BRHP has conducted these trainings and reviews with Yahoo! employees in a number of locations and functions, including the legal teams in the U.S., Latin America, Europe, Middle East and Africa (EMEA) and Southeast Asia, the global security team, customer care teams in Southeast Asia and the Middle East, and the product and editorial teams in the Middle East
- The BHRP conducts Human Rights Impact Assessments (HRIA) to identify circumstances when freedom of expression and privacy may be jeopardized or advanced. The BHRP conducts short-form HRIAs for specific, targeted questions or requests to review. Where Yahoo! identifies significant risks to users' free expression and/or privacy, however, it undertakes a long-form assessment. The long-form HRIA provides a comprehensive background on the business plans, human rights issues, potential risk mitigation strategies, and other relevant information. There are a variety of circumstances that trigger an HRIA, including:
  - review and revision of internal procedures for responding to government demands for user data or content restrictions in existing markets
  - entry into new markets

## CASE STUDY

In Vietnam, Yahoo! conducted a human rights impact assessment, which enabled the company to tailor its business operations to be consistent with its corporate human rights commitments. In that instance, Yahoo! decided to manage and operate Yahoo!'s Vietnamese language services out of Singapore so the services would be governed by laws with stronger protections than those in Vietnam today. The HRIA process also enabled the company to create legal structures, internal policies, user terms of service and tailored approaches on data access and location to protect its users and employees.

- launch of new products or services that may impact users' rights to privacy or free expression
- data storage decisions
- review of the free expression and privacy-related policies, procedures and activities of potential partners, investments, suppliers and other third-parties.
- The BHRP maintains an internal, restricted-access wiki that stores HRIAs, and internal requests to review transactions and business decisions
- In partnership with the Laogai Research Foundation, Yahoo! has created a Human Rights Fund to provide humanitarian and legal support to political dissidents imprisoned for expressing their views online, as well as assistance to their families.
- Yahoo! employees who receive government demands must escalate potential human rights issues to the BHRP
- Yahoo! discloses information only as required by applicable law; disclosures must be minimized
- Employees with access to personally-identifiable user data must protect the data from unauthorised access
- Yahoo! must respond to government requests for user data and content restrictions in a transparent manner.

Yahoo! has created a set of Global Principles and Procedures for government demands relating to user data and content restrictions that impact free expression and privacy. The principles state that:

- Government demands must be in writing, except where applicable law permits verbal demands, or in cases of emergencies
- Government demands must be made by authorized officials
- Senior Yahoo! executives have engaged with representatives of the Council of Europe and members of the European Parliament, as well as a number of U.S. government officials, among others, on issues relating to online freedom. In particular, Yahoo! has advocated for the release of those who have been imprisoned for expressing their views online
- The BHRP has participated in various panels and dialogues, including before the UN Secretary-General on Business and Human Rights, to shape solutions to issues of free expression and privacy in the ICT sector

**“As technology evolves and the virtually universal state interest in regulating the ICT sector increases, the issues at the intersection of privacy, free expression and technology become ever more complex. GNI’s collective, multi-stakeholder approach is key to identifying better insights and implementing specific, concrete solutions.”**

— Ebele Okobi-Harris, Director, Business and Human Rights Program at Yahoo!

- Yahoo! has established two international academic fellowships at Stanford and Georgetown universities to advance work on the intersection of privacy, freedom of expression and technology. The Yahoo! International Journalism Fellowship Fund was established at Stanford University in 2006 to support the work of journalists from countries in which there are serious challenges to a free press. The Yahoo! International Values, Communications, Technology, and Global Internet Fellowship Fund was established in 2007 at Georgetown University and supports the education and research activities of an annual Yahoo! Fellow in Residence and two Junior Yahoo! Fellows. The Yahoo! Fellows come from around the world, from diverse sectors (including corporations, government, academia, and civil society), and are responsible for multi-disciplinary research that explores how diverse international values apply to the development and use of new communications technologies
- Yahoo! promotes dialogue on the issues of free expression and privacy in the online context through an exchange of ideas and shared learning among companies, governments, non-governmental organizations, investors, users and other stakeholders at its annual Business & Human Rights Summit
- Yahoo!'s BHRP website (<http://humanrights.yahoo.com>) provides a platform to engage the company's multiple stakeholders on privacy and free expression issues, to describe the program's work, and to elicit feedback from Yahoo! users
- Yahoo! has funded organizations and projects including the 2010 Global Voices Summit, the Committee to Protect Journalists, Business for Social Responsibility and the Center for Democracy and Technology.

In its process of implementation of GNI's Principles, Yahoo! has gleaned a number of important lessons:

- First, the support of Yahoo!'s senior leadership has been critical to its progress thus far implementing GNI's Principles
- Second, GNI must take the variability of the ICT sector into account. GNI properly allows companies to be flexible in selecting the methods and processes that they use to incorporate human rights responsibilities into their business operations. For Yahoo!, having a dedicated Business & Human Rights Program has allowed the company to focus on the creation of necessary processes and procedures and provides a single point of contact for internal and external stakeholders
- Third, active and collective engagement with governments is critical to addressing the complex problems that lie at the intersection of privacy, free expression and the ICT sector
- Finally, GNI's great strength is the breadth of its participating organizations. The complexity of issues facing GNI member companies is best addressed with active participation and input of multiple stakeholders. In addressing business concerns globally, Yahoo! has drawn directly on the regional expertise of fellow GNI participants in different situations, including Human Rights Watch, the Committee to Protect Journalists and the Berkman Center for Internet & Society at Harvard University.

# GNI: LESSONS LEARNED AND LOOKING TO THE FUTURE

Since GNI launched, the core issues we are seeking to address have gained prominence among policy makers, in the media, and on the agendas of Internet users globally. Cognizance of the complexity and interdependence of these issues is becoming more widespread. For example, Web 2.0 and social networking applications have been highlighted for their role in raising awareness of human rights abuses in developing countries. At the same time, technology companies have been criticized for selling telecommunications networks and equipment to regimes that use those technologies and hardware for surveilling political activists – but Web 2.0 services cannot operate in the absence of telecommunications networks that provide connectivity locally, nationally and internationally.

This example shows the inter-connectedness of ICT and underlines the importance of growing our company membership. We have learned this year from our dialogue with companies that some are interested, but not yet ready to join us. In 2011, we will reach out to companies to allow them to get to know us better, to inform our work, and to engage substantively with them. Other priorities for the year include:

- Growing our membership across all constituencies
- Undertaking the first assessments of current company members
- Establishing a regular review of the Principles and Implementation Guidelines to reflect our learning, and taking account of new issues as they develop and in anticipation of our future growth

**“Enlightened companies now understand that environmentally sustainable and socially responsible business practices are essential for long-term business success. Protecting free expression and privacy is equally important. If people don’t feel that their rights will be protected and respected by operators of the telecommunications services they depend on, trust will erode and so will the value of the networks. Companies that earn people’s trust around the world will be the long-term winners.”**

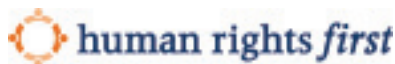
– Rebecca MacKinnon, Senior Fellow,  
New America Foundation

- Developing our internal learning program around the implementation of the Principles
- Establishing more structured channels for consultation with governments
- Further developing our institutional capacity within GNI.

Put simply, GNI is at the beginning of its work. Moving ahead requires thoughtful re-evaluation, incorporation of constructive criticism and strenuous effort.

**“Freedom House very much welcomes the work of GNI. Success should be judged according to the ultimate impact of policies on Internet use, especially in repressive environments. GNI needs to seek partners and members in Europe, Asia and Africa so that it is not seen just as a US initiative – but one that is truly global.”**

– Robert Guerra, Program Director, Internet Freedom, Freedom House



GNI is grateful for the legal advice and support it has received from White & Case LLP as it becomes established as an organisation.



## The Benefits of GNI Membership

- Build global public trust in your brand by demonstrating you care about users' rights around the world
- Manage company risk exposure and improve decision-making through GNI principles, guidelines, and the accountability process
- Engage in public policy as part of a diverse coalition
- Benefit from a unique opportunity to work through complex issues and learn in a safe space, gaining insight from other companies, civil society, investors and academic participants
- Demonstrate leadership in a critical area of social policy
- Influence a global standard for corporate responsibility in the ICT sector.

## To Find Out More

[www.globalnetworkinitiative.org](http://www.globalnetworkinitiative.org)



# The Global Network Initiative

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

