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

www.bsr.org

Commissioned by the Global Network Initiative

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.

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 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.

Contents

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[1] 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.

[1] 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.

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.

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.

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.

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:

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.[2]

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.

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.

[2] *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.[3]

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.

[3] See 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[4]

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.

[4] 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[5]

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	• 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. • End users are increasingly innovating with ICT products and services in unexpected ways that may be beyond company control.	• 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). • 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.
Legal Frameworks	• 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. • Governments around the world are making increasing demands—some positive and some negative—that impact human rights. • Laws that are enacted for ICT can sometimes conflict with internationally recognized human rights to security, privacy, and freedom of expression.	• 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. • In situations where local law conflicts with human rights, companies may need—or be expected to—challenge the law and its implementation. • Regulatory uncertainty or conflict between local law and international human rights standards can be barriers to private sector investment.

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

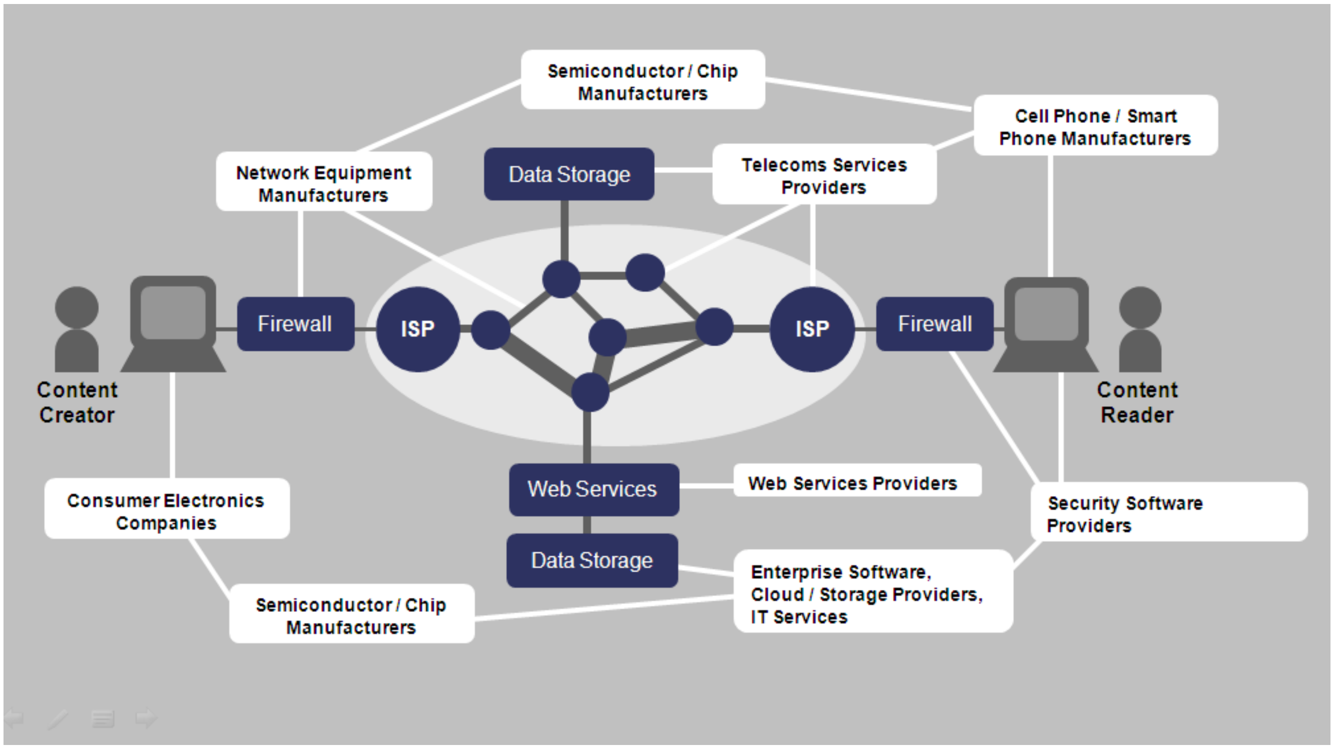
Jurisdictional Complexity	• The internet is global, but laws and regulations governing ICT companies are often national. • The evolutions in ICT use are raising important questions about legal jurisdiction, especially as data flows across international borders, is stored in multiple jurisdictions, or 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.	• 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.
Technological Complexity	• New technology can be complex to understand, and new product functionalities are rapidly introduced. • New products and services bring new risks and opportunities all the time, sometimes with unpredictable consequences. • Rapid global communications can magnify the impact and significance of important events and incidents.	• 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.
B2B and B2G: Relationships with Enterprise and Government Customers	• 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. • 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).	• 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.

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).


Semiconductor / Chip Manufacturers
Cell Phone / Smart Phone Manufacturers
Network Equipment Manufacturers
Data Storage
Telecoms Services Providers
Content Creator
Firewall
ISP
ISP
Firewall
Content Reader
Consumer Electronics Companies
Web Services
Web Services Providers
Security Software Providers
Data Storage
Enterprise Software, Cloud / Storage Providers, IT Services
Semiconductor / Chip Manufacturers

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 of 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.

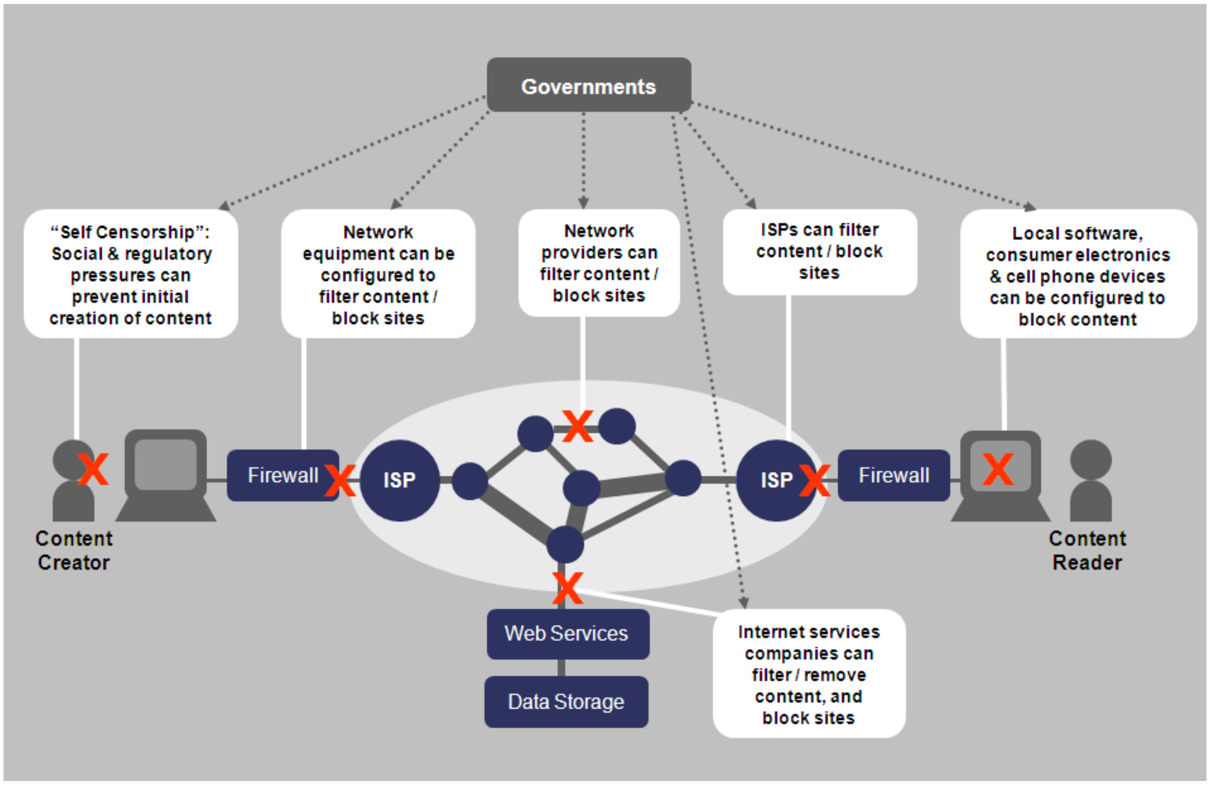
Governments are increasingly aware of the distinction; media reports suggest that governments are contemplating “technology-neutral” regulations, which would require all types of products and services that enable communications to be technically capable of providing information required by law enforcement agencies.[6] 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

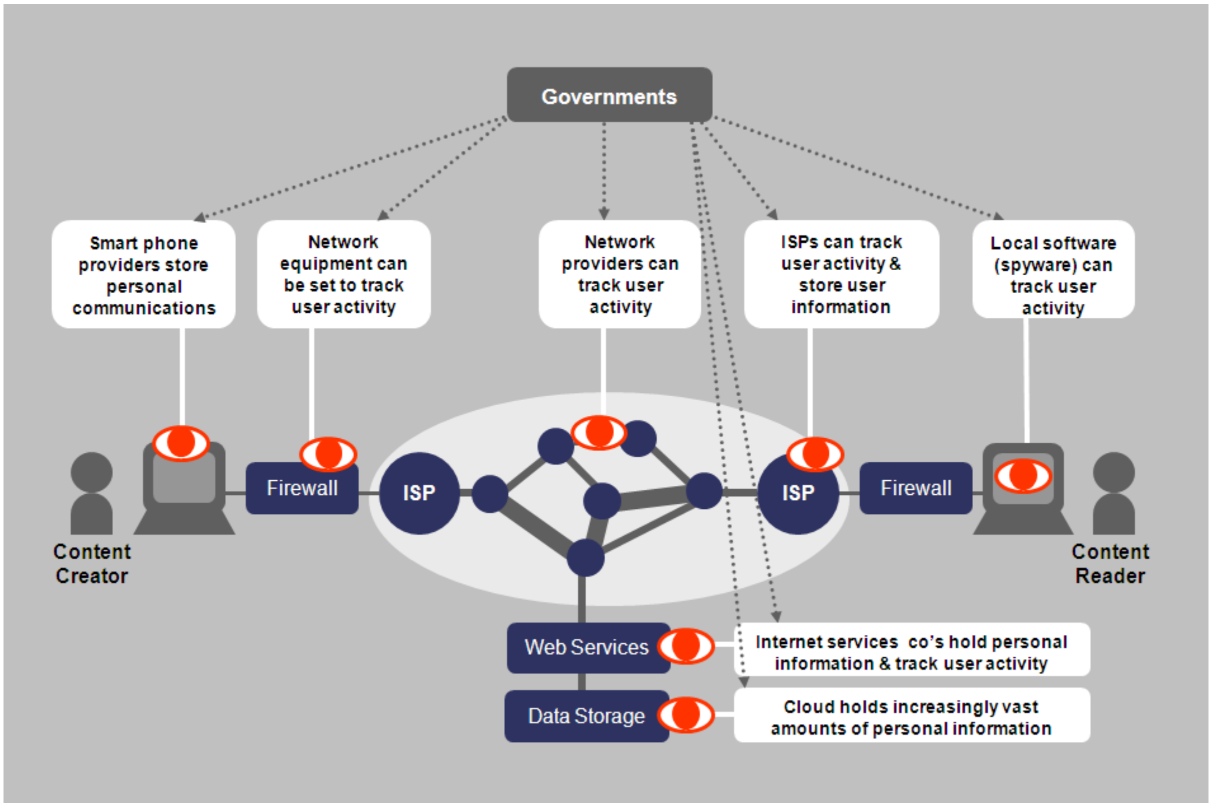
As can be seen from the accompanying diagrams, there are a number of different points across the ICT value chain in which governments can interact with private sector companies, sometimes at the level of content or personal information, and sometimes at the level of the product or service functionality. 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.

[6] *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


Governments
"Self Censorship": Social & regulatory pressures can prevent initial creation of content
Network equipment can be configured to filter content / block sites
Network providers can filter content / block sites
ISPs can filter content / block sites
Local software, consumer electronics & cell phone devices can be configured to block content
X
Content Creator
Firewall
ISP
ISP
Firewall
Content Reader
Web Services
Data Storage
Internet services companies can filter / remove content, and block sites

Privacy Risk Drivers Across the ICT Value Chain


Governments
Smart phone providers store personal communications
Network equipment can be set to track user activity
Network providers can track user activity
ISPs can track user activity & store user information
Local software (spyware) can track user activity
Content Creator
Firewall
ISP
ISP
Firewall
Content Reader
Web Services
Data Storage
Internet services co's hold personal information & track user activity
Cloud holds increasingly vast amounts of personal information

Summary of Human Rights Risk Drivers Across the ICT Value Chain	
ICT Industry Segment	**Key Freedom of Expression and Privacy Risk Drivers**
Telecommunications Services	• Companies hold vast amounts of personal information (call records, caller locations, etc.) and law enforcement agencies may demand access to it • 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 • 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. • 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.
Cell Phones / Smart Phones	• 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 • 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 • Software/hardware functionality can be configured to allow law enforcement agencies access to user communications, which can sometimes be used for privacy-invasive purposes
Internet Services	• 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. • Internet services companies can receive demands from governments to release personal information, such as emails, web surfing habits, etc. • There is pressure for internet companies to be held increasingly liable for user-generated content carried over their services (known as "intermediary liability")
Enterprise Software, Data Storage, and IT Services	• 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 • 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 • 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
Semiconductors and Chips	• Hardware can be configured to allow law enforcement access for surveillance • 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

Network Equipment	• 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 • 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
Consumer Electronics	• Governments could demand that computer manufacturers pre-install filtering and/or monitoring software designed to restrict access to content and/or allow for surveillance
Security Software	• Filtering software can be used by governments and/or other companies to restrict content in ways that infringe on rights to freedom of expression • Governments could demand that filtering software restricting freedom of expression is pre-installed in computers and/or mobile devices • 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 • Governments may prohibit the use of strong forms of encryption or demand that companies offer simpler means for encrypted information to be unscrambled

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.[7]

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).[8]

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

[7] 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

[8] 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

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.

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.

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?

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?

- 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:

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.

- 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.

- 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.