# ICT AND HUMAN RIGHTS

An ecosystem approach

# CONTENTS

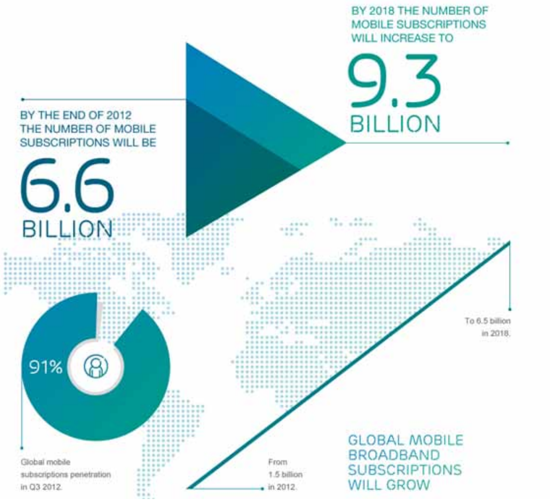
# INTRODUCTION

In our connected century, information and communication technology (ICT) is deeply integrated into our working and personal lives. Digital communication is more global, affordable and accessible than ever before, enabling billions of people to share ideas, acquire knowledge, improve their quality of life, and boost livelihoods. Many studies show a strong correlation between ICT and GDP growth.[1] ICT also promotes greater transparency and enhances many fundamental human rights – such as the right to health, education, freedom of assembly, and freedom of expression.

By 2017, it is estimated that 90 percent of the world's population will have 3G coverage; 50 percent will have 4G coverage, and by 2018, smartphone subscriptions will exceed 3 billion. By the end of 2012, mobile subscriptions reached 6.6 billion, and by the end of 2018, they are expected to reach 9.3 billion, with global mobile data traffic set to grow 12 times between 2012 and 2018.[2] For many, the mobile phone will be the only means of accessing the internet. Social media is booming: some 66 percent of online adults are connected to one or more social media platforms.[3] Every day, Twitter users send 175 million tweets.[4]

## Access anywhere, anytime, for anyone

The scale and speed of this transformation is unprecedented. Mobile broadband constitutes a social revolution of at least the same magnitude as railroads, electricity and automobiles. An average smartphone with 3G or 4G access has for all practical purposes unlimited processing power, data storage, access to human knowledge and global exchange of views. This is because increasingly these capabilities reside in "the cloud" (or the internet) rather than in the device, a simple example being, photo-sharing sites like Flickr.



The evolving Networked Society, in which anything that can be connected will be connected, offers tremendous potential. Examples include cars communicating with other cars, traffic surveillance systems for road safety and energy conservation through smart grids.

That in just five years more than three-quarters of the world's population will enjoy these opportunities, whether they live in a rural area in a developing country or urban center, makes mobile broadband the first truly global technology revolution. The ambition must be to protect and drive this evolution ensuring its global coverage and accessibility by all.

## Weighing the balance

A development of this significance carries a number of implications for society. The very potential of ICT to be integrated into nearly every facet of our lives poses serious societal challenges and ethical dilemmas – in

[1] Arthur D. Little (2011). Socioeconomic effects of broadband speed. Research project, Stockholm: Arthur D. Little; Press release September 27, 2011: A 2011 report, conducted jointly by Ericsson, Arthur D. Little and Chalmers University of Technology in 33 OECD countries, quantifies the isolated impact of broadband speed, showing that doubling the broadband speed for an economy increases GDP by 0.3 percent. http://www.ericsson.com/networkedsociety/media/hosting/Need_for_speed.pdf

[2] http://www.ericsson.com/res/docs/2012/ericsson-mobility-report-november-2012.pdf

[3] http://www.ericsson.com/res/docs/2012/consumerlab/tv_video_consumerlab_report.pdf

[4] http://internet-market-news.blogspot.com/2012/07/about-twitter.html

particular, regarding internet security, privacy, integrity and the protection of human rights in the use of ICT.

At a time when enormous databases are being built as a by-product of social media and the internet (a trend known as “big data”), questions arise as to who should have access to these databases, and to what extent the individual should have a right to know what information is distributed about them, to whom, and how it is used.

One of the main purposes of ICT is to foster the free exchange of views and information – which supports human rights such as freedom of expression, freedom of assembly, and the right to privacy. The same technology can also be used by governments to fight crime, assist in emergencies, but in some cases it can also be used to restrict human freedom. Today this restriction is relatively small but likely to grow as concern around cybersecurity is accelerated.

Through better understanding of the complex inter-relationships between members of the ICT ecosystem, it becomes easier to map the boundaries of responsibilities and possible courses of action. By engaging with the entire industry as well as focusing on their own power to influence and shape the debate, ICT companies can better identify concrete steps that each actor in the chain can take to avoid or mitigate human rights risks. Clearly defining respective roles and responsibilities is critical for developing a successful ICT ecosystem-wide approach in respect of human rights.

## Ecosystem gives the full picture

To avoid adverse human rights outcomes and to ensure that the positive benefits of ICT are fully realized, this challenge is best framed from an ecosystem perspective: that is, the many actors that provide ICT and its related products and services, and those who benefit from it – consumers and civil society. In this way, we can more easily understand the boundaries of responsibility, as well as the measures, actors can take to mitigate the human rights impact of misuse of the technology by governments. (See section III: The ICT ecosystem.)

## No easy answers

This paper is intended as a springboard for constructive multi-stakeholder dialogue about ICT and human rights – with particular focus on identifying emerging challenges such as in the areas of freedom of expression, freedom of assembly, data privacy and security and the relationship with law enforcement agencies. It is not intended to address the full range of human rights impacts for the ICT industry, such as conflict minerals, labor rights, and access to health or education.

There are no hard and fast answers to the rapidly emerging ethical challenges around ICT. Instead, this paper seeks to frame the key questions facing society:

- How can ICT’s positive role in fulfilling human rights be enhanced and its misuse by governments minimized?
- What measures can prevent and mitigate governments’ misuse of ICT without inhibiting the opportunities afforded by the rapid growth of ICT?
- What core expectations do stakeholders have of the ICT sector in respecting and enabling human rights and minimizing unintended consequences – and can the industry deliver in this respect?
- What are the roles and responsibilities of each member of the ICT ecosystem and how can they best collaborate to promote positive human rights outcomes?

In examining these key questions, this paper intends to present a way forward in the discussion; to suggest the next steps for the industry and other actors in the ICT ecosystem, and to gain more clarity and direction in addressing these complex issues. The responsibility that all actors bear is to ensure that billions of people around the world continue to enjoy the opportunities afforded by ICT with the full support of human rights.

# HUMAN RIGHTS, GOVERNMENT AND SOCIETY

Broadband networks are intended by mobile operators and network equipment suppliers to enable people to communicate anywhere, at any time, from any device. However, as with most technologies, there is the potential for ICT to be applied by governments and others in ways for which it was not originally intended.

The unintended use of ICT to restrict or violate human rights presents a significant new ethical challenge for the entire ICT ecosystem and policymakers. There is rising stakeholder pressure for greater transparency, constructive discussion and clear guidance on good corporate conduct and due diligence on human rights as well as appropriate limits of government control over communication services.

Freedom of expression is not an absolute right, however. International human rights law recognizes that states may have legitimate reasons to place individuals or groups – for instance those involved in terrorism or various forms of severe aggression – under surveillance in accordance with due process of law, notably where their actions are suspected to be criminal. Likewise, governments have the authority to restrict freedom of expression in support of legitimate societal goals in limited instances.

For instance, law enforcement agencies may legitimately restrict human rights such as freedom of expression, and lawfully intercept and retain data, in order to preserve public safety and national security interests. Examples include cases where the rights of others are adversely affected: child pornography, hate speech, defamation, incitement to commit genocide, or for the protection of national security, public order or public health. In addition, first responders require information to identify locations in cases of emergency.

## Potential abuses

The problem arises when there are illegitimate uses of ICT by governments. Potential abuses by governments within the broad telecom sector include misuse of lawful intercept systems, government censorship (filtering or blocking), network shutdown, misuse of operator network information for surveillance, or the forced distribution of politically motivated messages via operators' networks.

Government demands for access to information and control over ICT networks and services are increasing worldwide. The World Conference on International Telecommunication in Dubai, UAE, in December 2012 showed how some governments seek support from the United Nations to assume more control over the internet. For example, in Australia, proposed reforms to national security law requiring telecommunications and internet service providers to retain user data for up to two years have generated substantial opposition and media debate.[5] The EU has had similar legislation, the Data Retention Directive since 2006.

Such demands can place the individual's right to privacy and freedom of opinion at risk.[6] When privacy is compromised by excessive surveillance, data retention or other activities, personal security and the right to freedom of expression can be undermined, jeopardizing other human rights.

The challenge is determining a reasonable system of checks and balances to ensure the protection of freedom of expression and other human rights.

[5] http://www.theaustralian.com.au/national-affairs/attorney-general-nicola-roxon-leaves-door-open-to-data-retention/story-fn59niix-1226464847896

[6] Information and Communication Technologies and Human Rights: *Report for the European Parliament Enlarged Bureau of the Subcommittee on Human Rights*, http://www.europarl.europa.eu/RegData/questions/reponses_qe/2011/010306/P7_RE(2011)010306(ANN)_EN.pdf

# HUMAN RIGHTS AND THE ROLE OF BUSINESS

The role of business in respecting and protecting human rights is covered by the UN Guiding Principles on Business and Human Rights,[7] unanimously endorsed in June 2011 by the UN Human Rights Council. These principles comprise the first widely accepted global standard on the respective roles of business and governments, with the aim of ensuring that companies understand their part in respecting human rights, both within their own operations and through their business relationships.

The three pillars of the UN Protect, Respect and Remedy Framework for Business and Human Rights are:

- the State duty to protect against human rights abuses by third parties, including business, through appropriate policies, regulation, and adjudication
- the corporate responsibility to respect human rights, which means avoiding infringing on the rights of others and to address adverse impacts that occur; and
- greater access by victims of human rights abuses to effective remedy, both judicial and non-judicial.

Thus, the primary focus of the UN Guiding Principles is to ensure businesses respect human rights by taking action to avoid infringing on human rights and addressing any adverse impacts that arise. The Guiding Principles are voluntary and do not create any new legal obligations for states or business; they provide guidance on how these constituents can better meet their responsibilities in line with existing human rights standards, as well as identifying gaps where improvements can be made.

Several initiatives have emerged to provide more detailed sector-specific guidance on meeting these principles. At government level, the European Commission has established a project to provide guidance to the ICT sector on the corporate responsibility to respect human rights.[8] Industry initiatives include the Working Group on Human Rights of the Global e-Sustainability Initiative (GeSI),[9] the Global Network Initiative (GNI),[10] the Electronic Industry Citizenship Coalition (EICC),[11] and the Industry Dialogue.[12]

For all these groups, a key priority is determining how the actors within the ICT ecosystem can best share responsibility in respect of human rights, and work together to enhance the positive impacts and minimize the negative impacts of the misuse of ICT by governments.

[7] http://shiftproject.org/sites/default/files/GuidingPrinciplesBusinessHR_EN.pdf
[8] http://www.ihrb.org/project/eu-sector-guidance/index.html
[9] http://www.gesi.org/
[10] http://www.globalnetworkinitiative.org/
[11] http://www.eicc.info/
[12] http://www.teliasonera.com/en/newsroom/news/2012/industry-dialouge

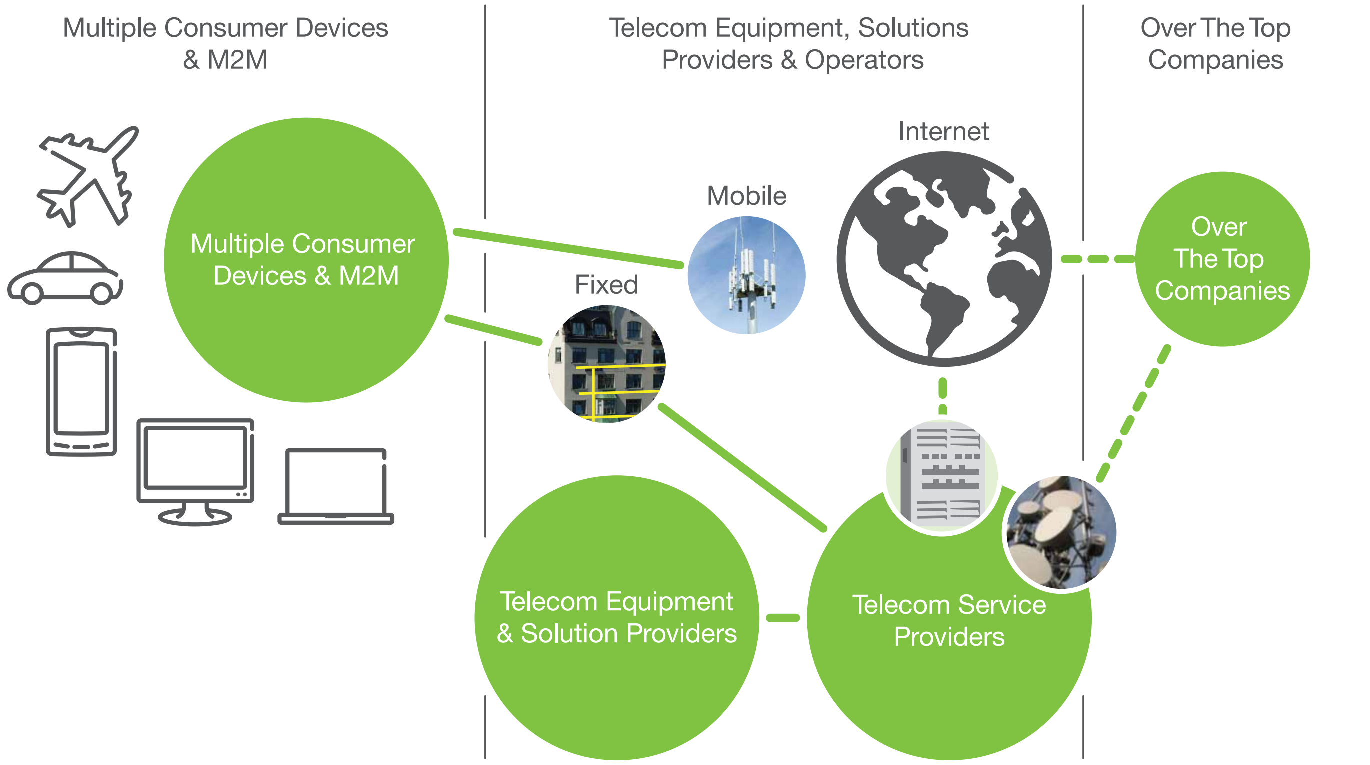
# THE ICT ECOSYSTEM

The different actors in the ICT ecosystem share a strong degree of inter-dependence. However, the type of human rights risks they confront – as well as their capacity to address them – may vary considerably, depending on their place in the value chain. For instance, companies may simultaneously be both suppliers and customers of telecommunications services and/or equipment, and many parts of the ICT ecosystem are global, trans-border and deregulated.

Understanding this web of inter-relationships can help identify the most significant human rights impacts and therefore the best opportunities for cooperation.

Given the complexity of the ICT ecosystem, below follows a simplified description of the major actors within the ecosystem, and some of the human rights impacts and risks that each faces.

## THE ICT ECOSYSTEM


Multiple Consumer Devices & M2M
Telecom Equipment, Solutions Providers & Operators
Over The Top Companies
Multiple Consumer Devices & M2M
Internet
Mobile
Fixed
Over The Top Companies
Telecom Equipment & Solution Providers
Telecom Service Providers

# ICT INDUSTRY ACTORS

### Telecom equipment and solutions manufacturers

**Role:** Provide fixed and wireless telecoms network equipment and solutions and software, such as switches, routers and radio base stations, as well as manage networks and provide related products and solutions.
**Potential Human Rights impacts:** Required by law to provide lawful interception capabilities, which can potentially be misused by governments. Tracking capabilities in the system of users ID and location may be misused by authorities, unlawful organizations and companies.

### Consumer electronic device providers

**Role:** Manufacture cell phones and other mobile devices, such as computers and tablets, enabling voice and data services. Location-based services available on mobile devices are generally designed to provide customer value. These services or apps, voluntarily downloaded by end users, can be used independently of network location services. Capabilities and control vary depending on the location functionality. It can be a feature of the terminal (GPS/GLONASS/Galileo receiver) and/or a (WAN/LAN) network feature (triangulation, etc.). Location data is extracted from the network or the device by the network operator or a third-party app/service provider.
**Potential Human Rights impacts:** Location-based information is also of great interest to law enforcement agencies. If used illegitimately or illegally, it presents risks to individual security and privacy.

Many (types of) apps and network services use location data from these functionalities. The “controller” of these apps/services is either a network operator or an OTT (over the top companies) service provider. Both can have human rights implications and can be abused by the operator/service provider or a government.

### Telecommunications services providers

(fixed and mobile operators)
**Role:** Provide local and international telecommunications services to users; both voice and data, including internet access. Can be legally required to assist law enforcement agencies by providing information regarding the identity or calling patterns of subscribers.
**Potential Human Rights impacts:** Misuse of lawful intercept systems included in operator networks, government censorship (filtering or blocking) of content, government orders for network shutdown, government surveillance to locate targets by misusing operator network information, forced distribution of politically motivated messages.

### Over the top companies (OTT)

**Role:** Internet service providers, enterprise and security software developers, IT service firms and content providers offer internet-based services, including search, e-mail, banking and commerce, social networking, content, location-based services, and weather information, and a wide range of applications; databases, storage and cloud computing; and software. A distinction could be made between service/app providers that provide an app that the user downloads to the device, as opposed to one native on their device or which uses a browser and thus resides entirely in the cloud.
**Potential Human Rights impacts:** Government censorship (filtering or blocking) of content, requests for user data, unclear or misguiding information on how data will be used and abuse of privacy and security with the download of location-based services. Companies may also use data that they collect on consumers and businesses in ways, which are not transparent, and can impact on rights, eg privacy.

User data can be contained in the device, in the service provider databases, as well as in the network, presenting human rights risks in terms of privacy and security. The location of servers and transport of information between countries may lead to unlawful interception and privacy issues.

### Third-party companies

**Role:** Offer applications (apps) in areas such as entertainment, business, health or education downloaded by consumers via marketplaces such as Apple Store and Google Play. Many app providers rely on the use of personal information to provide services to users.
**Potential Human Rights impacts:** Increasingly, data can be contained in the device, in the company databases, as well as in the network, presenting human rights risks in terms of privacy and security. Location of servers and transport of information between countries may lead to unlawful interception and privacy issues.

# GOVERNMENTS' ROLE IN ECOSYSTEM

## Governments

**Overall role:** Responsible for setting regulatory frameworks and establishing laws for the ICT industry, and to enforce national laws (which can in turn raise additional questions, for example about police intervention). Governments, have full sovereignty over their people and territory and, as such are the "ultimate controllers" of a country's communication services. Commercial ICT operators have a license to operate from the government. Despite widespread privatization of the telecoms industry, some operators are still wholly or partly state-owned. Government oversight primarily concerns services and content, not the equipment, and therefore impacts operators and service providers more directly than equipment vendors.

## Regulatory agencies

Governmental regulatory agencies ensure compliance with laws, regulations, and establish rules. This includes sector-specific regulators, general regulators (such as competition authorities), and special agencies or ministries charged with specific tasks (such as spectrum management). Their role may include:

- implementing the authorization framework that allows companies and investors to establish new ICT businesses and provide ICT services
- regulating competition
- regulating network inter-connection
- implementing universal service/access mechanisms to ensure the widespread (and affordable) diffusion of ICT
- managing the radio spectrum.

## Law enforcement

Law enforcement and first responders are integral to the government's role in the ICT ecosystem. Law enforcement requires access to certain information for the fulfillment of their duties while first responders require information to identify locations in cases of emergency.

## Standardization bodies

National, regional or international organizations produce voluntary standards (a set of rules or technical specifications for ensuring quality and interoperability) for the ICT industry.

**Potential Human Rights impacts:** Human rights issues may arise particularly in the areas of content or personal information, and product or service functionality, where government and private sector company responsibilities intersect. Potential abuses of the technology can occur, for example, in terms of censorship, excessive surveillance, blocking and filtering, and unwarranted access to communciations data (such as call logs and location data).

A government has a duty to protect the human rights of its citizens, while at the same time ensuring safety and security. However, their actions can also adversely impact the human rights of citizens, and this can vary in particular with regard to restrictive governments or governments in countries with weak human rights laws.

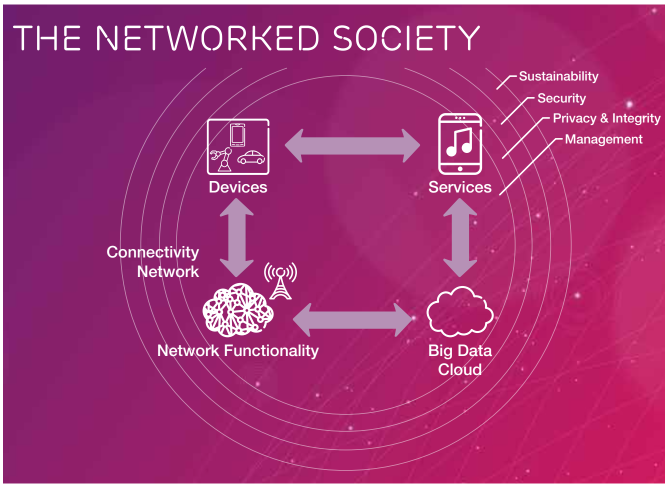
## Consumers and civil society

**Role:** Mobility is opening up the internet to more people every day, with new services for consumers; new ways for consumers and members of society, including industry, to interact with each other, and new ways for governments to interact with citizens.

**Potential Human Rights impacts:** Consumers have a personal responsibility as "netizens" to urge governments and companies to use ICT in a way that enhances open access and free speech.

# CHANGING LANDSCAPE OF ICT

The dynamic and rapidly evolving nature of ICT adds another layer of complexity. In the networked society the trend is from an operator-centric to a user-driven landscape redefining the network and connected devices as more data will be stored in the cloud and in the devices. As technologies continue to advance and the world becomes more digital, it will become even more challenging to ensure the protection of privacy and freedom of expression in the provision of services.


THE NETWORKED SOCIETY

The following section describes some key aspects of this changing landscape that will put increasing demands on management, security, privacy and integrity, and sustainability.

## Smartphones on the rise

As the telecom, IT and media industries converge, traditional networks are undergoing rapid change and evolution, and mobile networks are increasingly important and ubiquitous. One of the most dramatic changes is the rise of smartphones and tablets. Approximately 40 percent of all mobile phones sold in the third quarter of 2012 were smartphones, compared to around 30 percent in 2011. With only around 15 percent of worldwide subscriptions using smartphones, this figure is expected to grow.[13]

## Data explosion

Networks must handle increasing amounts of data. Today about 75 percent of all traffic is data, with online video representing 25-40 percent, followed by web browsing at 15-20 percent. LTE/4G advanced networks as well as heterogeneous networks with small cells, better frequency use and higher bandwidth will help meet requirements for high data rates.

## No spectrum without license

For telecom companies providing mobile services, the key distinguishing factor is the requirement for government licenses for spectrum that is necessary for providing telecom services. Operators need access to several different technologies and a significant amount of spectrum in various frequency bands to be able to provide a competitive range of services. Governments in each country want to ensure that sufficient spectrum is available to meet increased traffic demand on mobile broadband networks.

## The rise of cloud computing

Cloud computing is having a profound impact in digital communications. Network-supported cloud services offer efficient communications for high-quality video as well as advanced enterprise services. Today, almost all service development is taking place on the internet, with applications residing far beyond the telecom operators' domain.

The cloud benefits from a network that is service aware, and which provides other assets, such as security and authentication. This requires an opening of

[13] http://www.ericsson.com/res/docs/2012/ericsson-mobility-report-november-2012.pdf

the network towards potential service developers. As the ecosystem evolves and changes, over-the-top players will gain influence.

### New technologies

Two developments in particular may have a big impact on the telecom industry:

- HTML5 – the latest version of the standards used for displaying content and running applications from the web, aimed at making the internet the future platform for all services and applications
- WebRTC – a technology that allows developers to build real-time communication into web pages.

Unless the telecom industry can develop equivalent service-aware capabilities for applications developers, and continues to make traditional telecoms network apply new and modern web-based technologies, there is a risk that web-based services will be built completely outside the network – and outside the current regulatory environment.

# ICT AND HUMAN RIGHTS CHALLENGES

As ICT products and services – and the network of organizations that provide these – take on an increasingly important role in society, stakeholder awareness surrounding the possible risks that misuse of ICT poses to human rights is also growing. Three particular areas give rise to stakeholder concern: freedom of expression and assembly, data privacy and security, and the relationship with law enforcement agencies.

## Freedom of expression and assembly

Whenever internet services companies face demands from governments to remove, block or filter content, there is a risk that the human rights of freedom of expression and assembly may be violated.

This confers certain responsibilities on companies to respect these rights, often carried out through voluntary self-regulation of illegal content to maintain the openness of online communication.

The challenge is to clearly define such responses with transparency, accountability and in accordance with existing laws in order to uphold the procedural rights of internet users accused of violating the law.

## Data privacy and security

While data may be lawfully intercepted and retained by law enforcement agencies, protection of individual privacy and data security must be paramount.

Many companies have built robust security and privacy protections in their networks, but the adequacy of these protections will face increased scrutiny as data storage continues to grow. Future work in cyber security will need to address all network, terminal and application environments. From a standardization perspective, industry specifications on security architecture, protocols and networks will be increasingly important. Security must be a top priority in product development.

## Relationship with law enforcement agencies

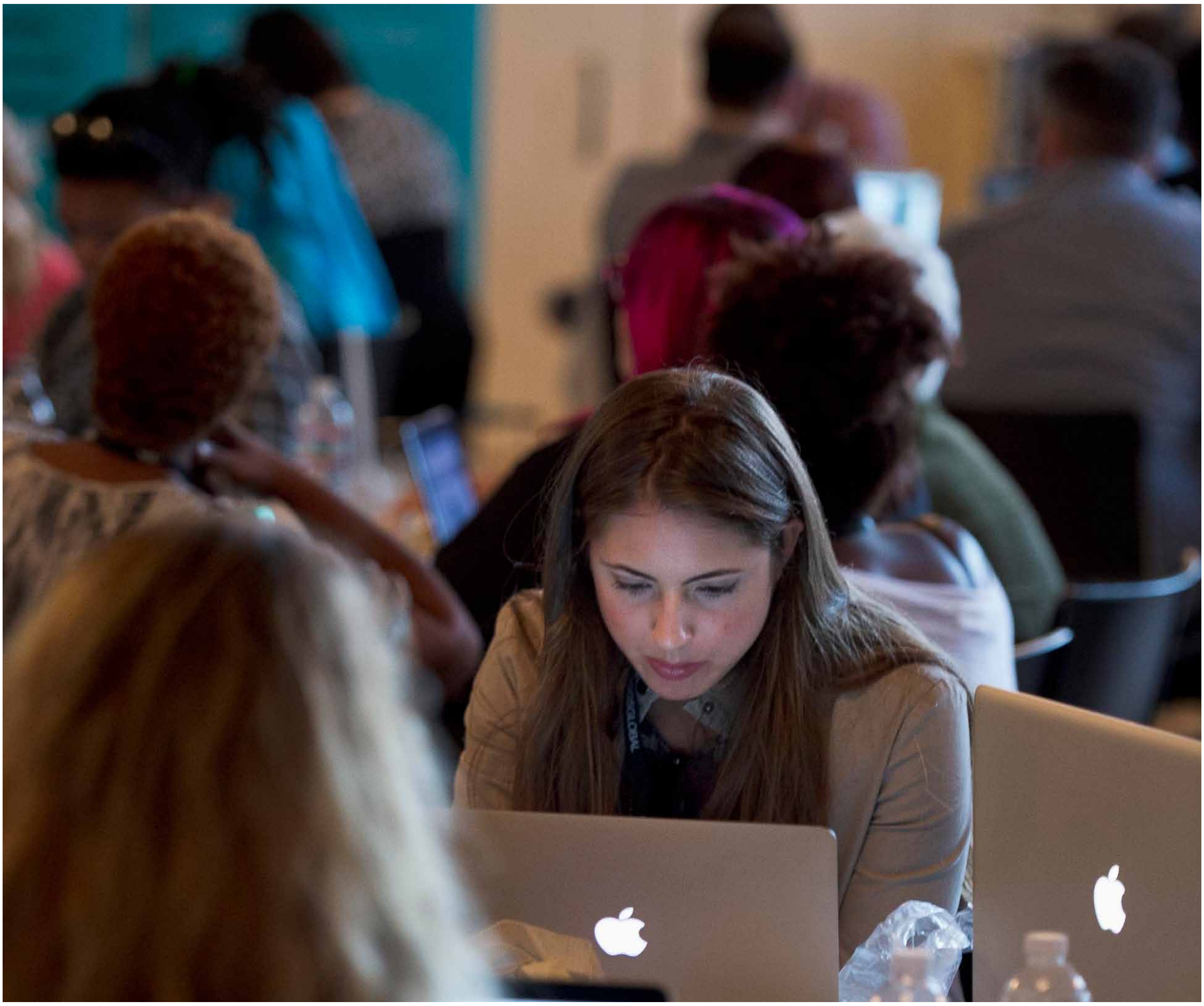
When ICT companies are required to assist law enforcement agencies in investigations, or face demands for information that go beyond normal practice or law, they can find themselves confronted with a dilemma: on the one hand they have an obligation to comply with local laws and assist in protecting public safety – and on the other they have a responsibility to respect the human rights of individual users and adhere to internal policies and procedures.

## Intended and unintended use of ICT

Telecommunications services include a variety of functionalities intended for either commercial or law enforcement purposes. In many cases, telecoms technology is mandated by law enforcement agencies to offer functionalities allowing for the removal, filtering and blocking of content, or which enable easier surveillance and access to personal information. In many countries these functionalities are regulated to ensure lawful, positive and beneficial use of this technology and to prevent misuse that could violate human rights. However, concern most often arises over possible misuse in countries with a poor human rights record.

**Lawful interception:** Lawful interception solutions are provided in markets where this constitutes a regulatory requirement. These solutions are based on international standards and allow, for instance, the ability to trigger on specific telecommunications identities, or individuals; the reporting to one or more law enforcement agency of specific events related to a target’s communications, and the option to retain data or transmit one or more copies of a communication session to law enforcement agency.

An unintended use can occur when an entity, such as a government, uses the feature to monitor the communications of citizens without the legal permissions that are required for such actions in other countries.



**Service-aware network:** A service-aware network is designed for commercial purposes, such as customer segmentation and proper billing, quality of service to the user/consumer and enables advanced network management, including detecting viruses as well as establishing appropriate costs to customers.

Certain technical functionalities within service-aware networks can and do enable detection by law enforcement agencies of illegal content, such as child pornography, hate or defamation propaganda.

Service-aware networks imply policy and ethical concerns in three main areas:

- the responsibility of the data processer or controller
- data privacy and protection
- third-country transfer (the transfer of personal data to another country).

The capability to closely inspect a packet of data can result in unintended use by individuals, authorities or governments who have not taken the proper legal steps to allow its use for that purpose. Security measures are embedded in the system to prevent misuse but it is difficult to ensure that these measures are fully effective in every instance, posing an ongoing challenge to the industry.

It should also be noted that service-aware capabilities are increasingly necessary to run networks. Additionally, a large amount of data is also collected in devices or handsets, and by many social media applications.

**Emergency response:** Basic positioning capability, on cell level, is necessary for call connection to function. Positioning supports a number of commercial services such as navigation services. It is also used for the monetization of services, such as enabling an operator to set charges based on market segmentation.

Most critical, however, is the role of positioning capability in emergency response. It enables radio traffic, telephony and data communication to be integrated in a single system so police and emergency personnel can detect callers' locations in the event of life-threatening emergencies and acute rescue situations. It means that police and rescue personnel can work in parallel, and in real time, within a single system to address an emergency situation.

However, while positioning information undoubtedly serves a vital role, its unintended use can raise privacy concerns, including the ability to be tracked without one's knowledge through location services. It should be noted that unintended privacy concerns can also arise in non-integrated systems.

**Mass transmission of information:** This functionality allows SMS messages to be sent to mobile phones by a government or organization, for example to issue warnings of natural disasters or other emergency events requiring immediate broadcast and delivery of simultaneous alerts to protect public safety.

An unintended use could be a government demand to use mass transmission for the purpose of sending out government propaganda.

**End-to-end encryption:** This is uninterrupted protection of the confidentiality and integrity of transmitted data by encoding it at its starting point and decoding it at its destination. It involves encrypting clear data at source with knowledge of the intended recipient, allowing the encrypted data to travel safely through vulnerable channels (such as public networks) to its recipient, where it can be decrypted (assuming the destination shares the necessary key-variables and algorithms).

With increased emphasis on information security, using encryption technology to protect communications becomes more important. An unintended consequence is when governments increasingly demand the means to more easily unscramble encrypted communications. In countries with poor human rights records, this could pose a risk to the protection of human rights.

Together, these functionalities are designed to maintain a reliable flow of information. When used for their intended purpose, they are supportive of human rights.

### Regulatory framework

The legal and regulatory framework plays an important role in protecting human rights within the ICT ecosystem.

Most national governments impose regulatory requirements on mobile operators operating in their country to ensure that the right to freedom of expression and privacy is respected, except in circumstances where others' rights are adversely impacted, or for reasons of law enforcement, crime prevention, or public safety.

To operate a telecommunications network, an operator must be issued with a license from the national regulatory authority in a particular country before gaining access to consumers. The mobile network also generally requires a license from the regulatory authority to use the radio frequency bands of the electromagnetic spectrum in a process known as frequency or spectrum allocation. The telecom industry is therefore highly dependent on national regulatory authorities for its license to operate.

On the other hand, the internet is essentially unregulated, with the exception of laws to prevent its use for child pornography, hate crimes or terrorism. The International Corporation for Assigned Names and Numbers (ICANN),[14] a non-governmental organization, coordinates the architecture and structure of the internet domain name system, while the Internet Governance Forum facilitates multi-stakeholder policy dialogue. Protocols and technical capabilities for coding information are unregulated.

Data privacy, however, is regulated in many countries and recently there has been much debate in a number of countries on the need for further safeguards.

[14] http://www.icann.org/

# FINDING THE BALANCE

Ensuring that ICT products and services do not adversely impact human rights or freedom of expression can be especially challenging for ICT companies in situations where governments – whose duty it is to protect citizens' human rights – seek to extend their use of ICT functionality in ways that repress or violate human rights.

Once operating in a country and bound by license agreements with a government, it can be difficult for an operator to refuse to comply with government requests; in addition to the human rights implications for users of the network, such a refusal could result in the business being shut down, or employees being put at risk. Where regulation or minimum standards are lacking or conflicting, ICT companies are increasingly expected to take a proactive approach to respecting freedom of expression and other related human rights. At present, however, there is no ICT sector-specific requirement or guideline on how a company should handle ethical challenges arising from misuse.

What companies can, and should do, in such situations is therefore an important topic for ongoing multi-stakeholder dialogue. One focus of ongoing discussion is the possibility of a voluntary industry code of conduct to provide guidance. The European Commission, for instance, has hosted a series of expert workshops and has a project underway to provide guidance on ICT and human rights.[15]

When the customer is a nation state, the ability of a company to influence is limited: if the state does not fulfill its duty to protect under the UN Guiding Principles, to whom does the company appeal? What are its options and responsibilities? The UN Guiding Principles make it clear that business is not expected to take over the state's role in protecting human rights. But does the company's responsibility to respect rather than protect human rights change in this scenario?

Confronted with an ethical dilemma around human rights, a company faces a number of choices. This can include trying to persuade a government to change its conduct. If that is not successful, another alternative is to refuse to comply with requests that are in violation of human rights. A third option is pulling out of the market in question. The success of each of these will also be affected by the company's role in the ICT value chain, and of course on what leverage they actually have.

In such cases, a company must carefully weigh its role and responsibility. ICT has become an important vehicle for economic development, improved quality of life and the free exchange of information and ideas integral to democratic societies.  To close down a network – as long as it is operating in accordance with international sanctions and all other legal requirements – can do more harm than good by negatively impacting freedom of expression and other human rights for that country's citizens.

To navigate these difficult ethical dilemmas, it is vital for companies to have comprehensive internal policies aligned with UN human rights guidelines and other internationally accepted standards and guidelines, as well as procedures in place across their global business operations. Because the ICT ecosystem is so complex, each company must examine its own upstream and downstream operations and undertake the necessary due diligence to comply with its human rights obligations.

## Good governance and guidance

An effective human rights corporate governance framework starts with a commitment to respect human rights across a company's global business operations. This should be accompanied by human rights due diligence to identify risks and opportunities in different markets as well as policies and processes to address issues that arise.

[15] http://www.ihrb.org/project/eu-sector-guidance/index.html

## Corporate commitment

The commitment to respect, protect and remedy human rights starts at the top – with senior management commitment to align business conduct with internationally recognized human rights standards, such as the Universal Declaration of Human Rights (UDHR). A number of responsible business frameworks – such as the United Nations Global Compact – include such a commitment (see below).

## Due diligence

Every member of the ICT ecosystem, regardless of its place in the value chain, has an obligation to conduct adequate due diligence of its operations to assess and evaluate their human rights impacts and risks to ensure it is not infringing on human rights.

Due diligence and decision-making processes should include consideration of human rights, including upstream suppliers in the ecosystem. Conducting human rights due diligence is a requirement of the UN Guiding Principles, along with:

- having a human rights policy
- assessing actual and potential human rights impacts
- integrating findings across the company
- tracking and communicating performance.

## Policies and processes

Company-wide policies and processes for managing compliance – with local and international human rights standards, relevant export, customs, trade or labor laws and regulations, business and human rights frameworks and international sanctions – is a vital element of good corporate governance on human rights.

With processes in place to ensure compliance with all relevant internal policies and external requirements, any use of technology that violates applicable laws or has a detrimental effect on human rights, can be prevented or quickly detected, addressed and remedied. An effective internal assessment mechanism can also be a further safeguard to ensure compliance with sanctions, export control regulations and other requirements.

There are a number of helpful frameworks to help companies design and implement a robust system of corporate governance for human rights.

## Frameworks to guide business and human rights

Many frameworks exist to help business fulfill its human rights responsibilities – including the OECD Guidelines for Multinational Enterprises,[16] the UN Global Compact Principles[17] and the UN Guiding Principles on Business and Human Rights[18] (see page 7). Common to all of these is the fundamental recognition of a state's duty to protect the human rights of its citizens.

Among the most widely used standards for due diligence in human rights, in addition to the OECD Guidelines, are the new International Standards Organization's ISO 26000,[19] the standards of the International Finance Corporation,[20] the European Union's new strategy on corporate social responsibility,[21] and specific provisions of the US Dodd-Frank Act.[22]

## Need for continued dialogue

As our understanding of the increasingly important interrelationship between ICT and human rights matures, stakeholder expectations are evolving rapidly over the role ICT companies can and should play.

[16] http://www.oecd.org/daf/internationalinvestment/guidelinesformultinationalenterprises/
[17] http://www.unglobalcompact.org/aboutthegc/thetenprinciples/index.html
[18] http://www.business-humanrights.org/SpecialRepPortal/Home/Protect-Respect-Remedy-Framework/GuidingPrinciples
[19] http://www.iso.org/iso/home/standards/management-standards/iso26000.htm/
[20] http://www1.ifc.org/wps/wcm/connect/topics_ext_content/ifc_external_corporate_site/ifc+sustainability/publications/publications_handbook_pps
[21] http://ec.europa.eu/enterprise/newsroom/cf/_getdocument.cfm?doc_id=7010
[22] http://www.sec.gov/about/laws/wallstreetreform-cpa.pdf

In recognition that ICT and human rights challenges are complex and fast moving, with little precedent to draw on, a number of important recent events on business and human rights have highlighted the need for continued dialogue.

Among these was the ministerial conference on internet freedom held in The Hague, the Netherlands, Freedom Online – Joint Action for Free Expression on the Internet,[23] attended by representatives of over 20 countries, international organizations and private sector representatives. The conference sought to facilitate a global dialogue about the responsibilities of governments from around the world with an interest in proactively furthering human rights on the internet, in close engagement with companies, NGOs, and representatives of international organizations. A group of countries established a coalition for internet freedom, and jointly endorsed an outcome declaration[24] that called for, among other things, a multi-stakeholder process to further internet freedom globally and pledged to engage with the ICT sector, to encourage businesses to adopt practices, policies and principles that address concerns related to human rights and ICT.

## Sector-specific guidance

In the medium term, we expect continued dialogue and collaboration involving the various players in the ICT ecosystem to result in the development of sector-specific guidance on human rights.

In 2012, dialogue has continued in a number of forums, including the Stockholm Internet Forum on Internet Freedom for Global Development,[25] the EU Presidency Expert Conference on Business and Human Rights in Copenhagen,[26] and the European Commission's Roundtable on business and human rights.[27] The EU is currently developing sector-specific human rights guidance on implementation of the UN Guiding Principles on Business and Human Rights, with the ICT sector among the selected sectors.

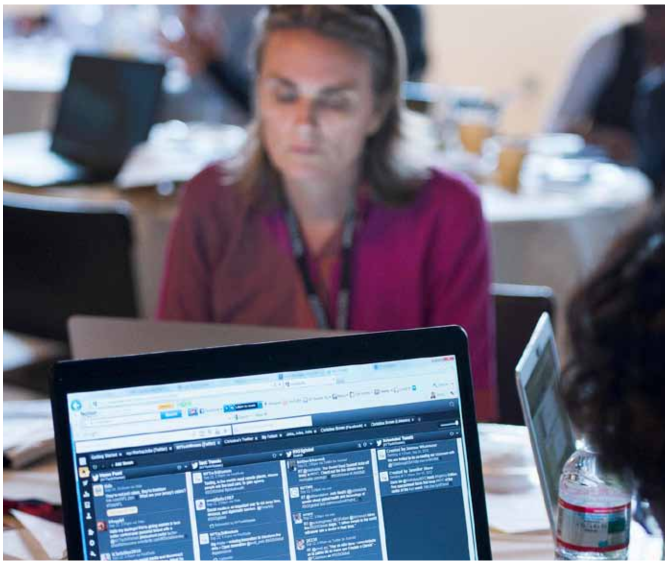
It is hoped that such guidance will help clarify the various roles and responsibilities of different players in the ICT ecosystem, identify areas for collaboration, and highlight how the positive impacts of ICT can be maximized.

[23] http://www.minbuza.nl/en/ministry/conference-on-internet-freedom
[24] http://www.minbuza.nl/binaries/content/assets/minbuza/en/the_ministry/declaration-final-v-14dec.pdf
[25] http://www.stockholminternetforum.se
[26] http://eu2012.dk/en/Meetings/Conferences/Maj/Foerste-til-femtende/Business-and-Human-rights
[27] http://www.ihrb.org/project/eu-sector-guidance/consultation-documents-and-reports.html

# CONCLUSION

Any potential risk or harm from use of ICT must be weighed against the tremendous benefits of the technology to advance and protect human rights. The internet and mobile communications have dramatically changed our world and the way we communicate, connecting billions of people around the globe, shaping new opportunities for collaboration and exchange of ideas. ICT has empowered people to more fully realize their human rights, from freedom of expression and freedom of assembly, to economic, social and cultural rights that enable, for example, greater financial inclusion through new markets for trade and commerce and improved access to health and education.

Certainly, the relationship between human rights, ICT, law enforcement and national security is complex. At one end of the spectrum, this extraordinary technology delivers connectivity, empowerment and contributes to more transparent, safer societies. At the other end, unmitigated, unintended use of ICT can result in persecution, repression and human rights violations. This paper has sought to highlight this tension and lay the foundations for an ICT human rights framework that can harness the technology for good.



There are several considerations in the ongoing dialogue to develop a better understanding of the implications of ICT's impact on human rights and the responsibilities of each member of the ICT ecosystem to address these implications in respect of human rights:

- protecting the internet as a place for the free exchange of views and information
- driving global standardization and other initiatives that can reduce the economic threshold for private and business enterprise
- supporting education over the internet for sustainable economic growth
- countering misuse of the internet and social media through increased user insight and transparency
- monitoring trends in the digital global community, for example big data, social media, the Internet of Things and selective information access, to identify and act on unwanted side-effects without suppressing the evolution of ICT
- establishing robust human rights impact assessment capabilities and due diligence processes within companies.

## A multi-stakeholder approach

While individual company responsibility is paramount, the ethical challenges surrounding human rights and ICT must also be addressed through a multi-stakeholder approach. Developing effective and enduring solutions requires the cooperation of a wide range of stakeholders, all players within the ecosystem, as well as local and national governments, international bodies, business partners, human rights NGOs and other representatives of civil society.

Through better understanding of the complex inter-relationships between members of the ICT ecosystem, it becomes easier to map the boundaries of responsibilities and possible courses of action. By engaging with the entire industry as well as focusing on their own power to influence and shape the debate, ICT companies can better identify concrete steps that each actor in the chain can take to avoid or mitigate human rights risks. Clearly defining respective roles and responsibilities is critical for developing a successful ICT ecosystem-wide approach in respect of human rights.

### Avenues for collaboration

The UN Guiding Principles encourage businesses to achieve greater influence through capacity building and collaboration with other actors. This is a particularly promising avenue for the ICT industry, given the interconnected nature of the ecosystem. Expanding existing collaborative efforts and creating new ones will accelerate the industry's progress on addressing human rights.

Among the initiatives already addressing this is the human rights working group of the Global e-Sustainability Initiative (GeSI), formed in May 2012, with the objectives of:

- creating a broader understanding of the ICT ecosystem and its implications for human rights
- sharing information on latest developments in business and human rights, with particular emphasis on privacy and freedom of expression
- discussing practical means of implementing the new UN Guiding Principles on Business and Human Rights in the ICT sector
- coordinating GeSI's involvement in the European Commission's project to develop human rights guidance for the ICT sector
- creating a broad, multi-stakeholder group that can openly discuss challenges and solutions to ICT and freedom of expression issues.

Through such initiatives, the sector can help to drive pro-human rights agendas and industry best practice in the ICT ecosystem as a whole. Nonetheless, the rapid development and uptake of the technology and the unpredictability of future applications means this field will continue to evolve.

Multi-stakeholder collaboration should focus on several issues, including how to use ICT to enhance human rights and the public good; the necessary actions to minimize misuse; the types of regulation and standardization that will offer adequate safeguards while allowing the necessary flexibility for a rapidly evolving sector; how to best address stakeholder expectations, and how to ensure successful ICT ecosystem collaboration for positive human rights outcomes.

Taking action now to embed the ICT ecosystem upon a sound human rights foundation is essential. With billions of people around the world using and benefiting from ICT, the actions and decisions the sector takes today will have profound human rights consequences for society in the future. As we evolve to an increasingly networked society, new ethical challenges will continue to emerge, highlighting additional areas to explore and underlining the importance of a unified and thoughtful industry response.

# RESOURCES

UN Guiding Principles of Business and Human Rights
http://www.business-humanrights.org/SpecialRepPortal/Home/Protect-Respect-Remedy-Framework/GuidingPrinciples

European Commission Discussion paper on human rights due diligence guidelines
http://www.ihrb.org/project/eu-sector-guidance/consultation-on-sector-discussion-papers.html

Global Network Initiative (GNI) Principles
http://www.globalnetworkinitiative.org/principles/index.php

AccessNow Telco Action Plan
https://s3.amazonaws.com/access.3cdn.net/1f9ab2891a86f3f081_uom6iil1w.pdf

Protecting Human Rights in the Digital Age, Business for Social Responsibility
http://www.bsr.org/our-insights/report-view/protecting-human-rights-in-the-digital-age

Applying the UN Guiding Principles on Business and Human Rights to the ICT Industry
http://www.bsr.org/reports/BSR_UN_Guiding_Principles_and_ICT.final.pdf

Ericsson is shaping the future of mobile and broadband internet communications through its continuous technology leadership.

Providing innovative solutions in more than 180 countries, Ericsson is helping to create the most powerful communication companies in the world.

The content of this document is subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document

Ericsson AB
SE-126 25 Stockholm, Sweden
Telephone +46 10 719 00 00
Fax +46 8 18 40 85
www.ericsson.com