Telecommunications and Human Rights

An Export Credit Perspective

IHRB

Telecommunications and Human Rights

An Export Credit Perspective

February 2017

Cite as: Institute for Human Rights and Business, "Telecommunications and Human Rights: An Export Credit Perspective" (February 2017).

Attribution: The paper is written by the Institute for Human Rights and Business with contributions from Johan Henningsson, SEK; Karl-Oskar Olming, EKN.

About this Paper

In 2014, The Swedish Export Credits Guarantee Board (EKN) and the Swedish Export Credit Corporation (SEK) approached the Institute for Human Rights and Business (IHRB) to produce a paper on the human rights benefits and challenges of financing telecommunications exports in order to further develop their own due diligence for telecom transactions. The paper is written by the Institute for Human Rights and Business with contributions from Johan Henningsson, SEK; Karl-Oskar Olming, EKN.

This paper focuses on export credits granted to the telecommunications sector by EKN and SEK, the organisations involved in Sweden's export credit system. EKN and SEK's mission, as established by the Swedish Government, is to support the Swedish Export industry in a sustainable way worldwide.

IHRB

Founded in 2009, IHRB is the leading international think tank on business and human rights. IHRB's mission is to shape policy, advance practice and strengthen accountability in order to make respect for human rights part of everyday business. | www.ihrb.org

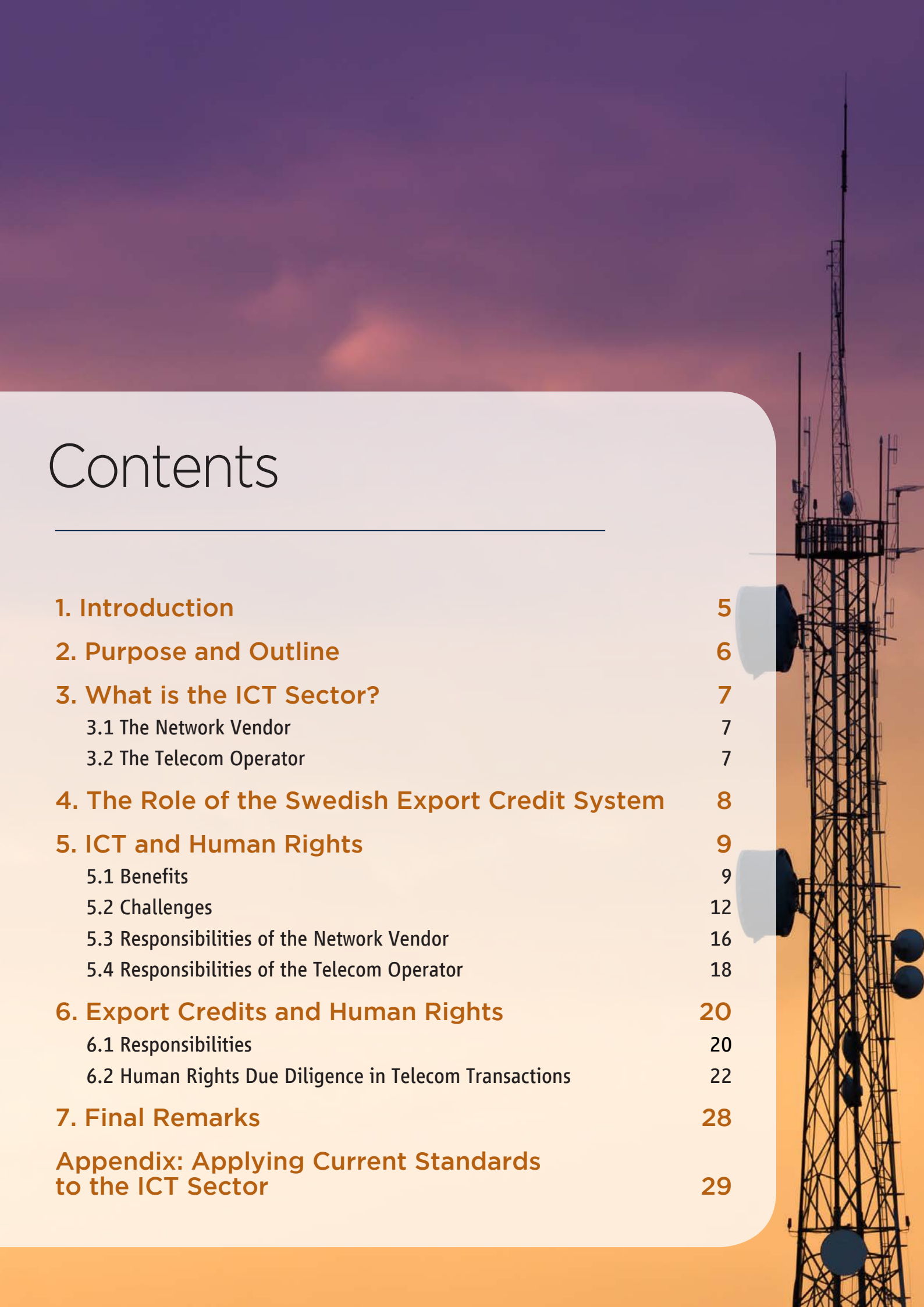
Swedish Export Credits Guarantee Board (EKN)

EKN is an agency commissioned by the government to promote Swedish exports and the internationalisation of Swedish companies. EKN insures payments and financing to make it easier for a bank or exporter to offer credit to the buyer of Swedish exports. EKN's clients cover a number of sectors and range from large multinational to small local enterprises. EKN is financed with the premiums paid by guarantee holders.

Swedish Export Credit Agency (SEK)

SEK is a state-owned company with a mission to ensure access to financial solutions for Swedish export industry. SEK has a complementary role in the market and offers financing of export credits and other financial products to Swedish exporters, their subsidiaries and their customers in order for Swedish companies to grow, invest or win export contracts overseas. SEK arranges finance, often in partnership with Swedish and international banks. SEK is financed by issuing bonds on the international capital markets.

Contents



1 Introduction

Since the adoption of the United Nations Guiding Principles on Business and Human Rights (UN Guiding Principles) in 2011,[1] attention to the corporate responsibility to respect human rights in the Information Communication Technology (ICT) sector has increased. ICTs increase connectivity, enable communication and make significant contributions to socio-economic development. However, ICT technologies can also be used by governments to arbitrarily restrict freedom of expression and privacy of end users.

As more of these impacts are discovered by nongovernmental organisations (NGOs) and reported by the media, companies in the ICT sector are under greater scrutiny to answer to their board, shareholders and investors, as well as consumers, civil society organisations, and the wider public as to how they are building human rights considerations into design of products and services and how they are assessing risks to human rights. Moreover, companies themselves are taking more significant steps to assess and address human rights risks and opportunities in their operations.

The UN Guiding Principles are built on three main pillars:

- the state duty to protect human rights
- the corporate responsibility to respect human rights
- the need to provide access to remedy

The corporate responsibility to respect human rights applies to all business sectors, regardless of their geographic location. The UN Guiding Principles also refer to the responsibility of States to "take additional steps to protect against human rights abuses by business enterprises owned or controlled by the State, or that receive substantial support and services from State agencies such as export credit agencies and official investment insurance or guarantee agencies, including, where appropriate, by requiring human rights due diligence."[2]

Under an export credit system, loans and risk cover can be arranged for the domestic exporter's international customers. Providing loans to international customers promotes a country's export industry and reduces the risk of non-payment to domestic exporters. The Swedish export credit system consists of two organisations; the Swedish Export Credit Guarantee Board (EKN) and the Swedish Export Credit Corporation (SEK), each with a distinct function and operating under separate management. EKN insures payments and financing of export contracts and SEK provides long term financing. EKN is the official export credit agency (ECA) in Sweden while SEK is a state owned financial institution. The

1 Office of the High Commissioner for Human Rights, "UN Guiding Principles on Business and Human Rights: Implementing the 'Protect, Respect, Remedy' Framework" (2011), at: http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

2 UN Guiding Principle 4

telecommunications sector is an important sector in the Swedish export credit system.[3]

The UN Guiding Principles provide an important reference point and a driver for the Swedish Export Credit System, as well as their customers, to carry out their operations in a manner consistent with them. Furthermore, responding to the impetus created by the UN Guiding Principles and the development of the ICT sector, in 2011, the Government of Sweden included in its annual letter of appropriation to EKN a first-time reference to "freedom online" ensuring that the organisation take these issues into account when assessing potential transactions.

Purpose and Outline 2

This paper focuses on the telecom subsector, i.e. telecom vendors and operators, due to the fact that the Swedish export credit system deals primarily with financing of telecom operators. However, as the telecom sector is a part of the wider ICT sector, broader references to ICT are included as well where appropriate.

The purpose of the paper is to:

- Clarify the Swedish export credit system´s responsibilities under the UN Guiding Principles in telecom transactions
- Suggest principles for human rights due diligence for export credits in telecom transactions

The first two sections of the paper explain different actors in the ICT sector[4] and consider the role of the Swedish export credit system in financing telecom transactions. This is followed by an analysis of network vendors´ and telecommunication operators' human rights responsibilities based on the UN Guiding Principles, emerging international standards, and good practice examples, as well as observations about responsible technology and its potential use and misuse.

The concluding section proposes human rights due diligence principles for the Swedish export credit system supporting telecom exports.

3 For clarity of this paper, EKN or SEK do not support export of mass surveillance equipment or intrusion software. Consequently EKN or SEK does not have any customers, i.e. exporters, which supply such equipment. A definition of mass surveillance and intrusion software is provided on p. 11 (p14)

4 The ICT sector can be categorised in a number of ways. For examples, see: https://www.bsr.org/reports/BSR_Protecting_Human_Rights_in_the_Digital_Age.pdf; http://www.oecd.org/internet/ieconomy/44949023.pdf

What is the ICT Sector? 3

The ICT sector is made up of many types of companies delivering products and services. Understanding the role of each part of the sector, from network vendors and telecommunications operators to web-based services, manufacturers of end user devices, components, and software, is crucial in identifying boundaries of responsibility and potential adverse human rights impacts associated with companies in the sector. While acknowledging the sector's diversity, as well as increasing convergence of ICT devices and services, this paper focuses primarily on the human rights responsibilities of telecommunications network vendors and operators.

3.1 The Network Vendor

Network vendors typically build, and in some cases manage, the telecommunication infrastructure that provides the basis for all fixed and mobile communications, including calls and data. A network vendor ensures that connectivity can occur across services, operators, and borders, and is capable of handling the increasing demands for data and access. An example is the growing demand for new media on devices connected to the Internet. A network vendor's main customers are telecoms operators.

3.2 The Telecom Operator

Telecom operators are consumer-facing companies that provide mobile and Internet services. Telecommunications infrastructure is considered critical infrastructure for any country. As such, operators of telecommunications networks do business in a highly regulated environment and maintain ongoing relationships with governments in the countries where they operate, as they require a number of national and local licenses to build, maintain, and operate their services.

The Role of the Swedish Export Credit System

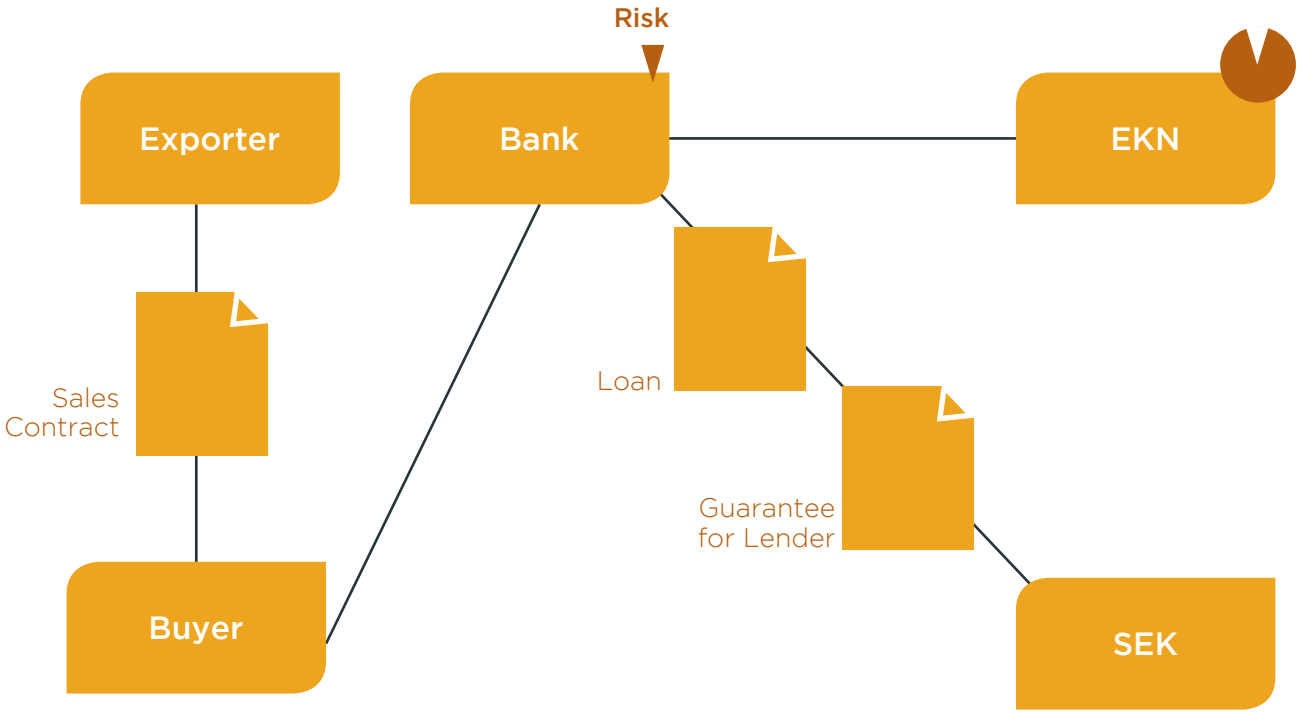
4

The Swedish Export Credit system facilitates financing of the buyers of Swedish exports. This can be seen, for example, in operators buying telecommunication network equipment. The Swedish Export Credit System generally does not have direct relationships with buyers. Instead, the system is positioned behind either the exporter or the commercial bank providing the loan.

EKN has a relationship with the vendor and/or the bank providing the loan, while the bank and SEK have a relationship with the operator in the form of a loan agreement.

The bank is normally fronting the transaction and has a direct business relationship with the operator, acting as SEK's agent. The bank negotiates the loan agreement with the operator and then the loan agreement is assigned to SEK. In this way, both EKN and SEK enter into the relationship with the operator, through the bank and after the loan agreement has been assigned.

Figure 1. The bank arranges the loan finance structure



ICT and Human Rights 5

The ICT sector fosters free exchange of views and information which support human rights. The same technology is used by governments to fight crime and assist in emergencies. However, in some cases this technology can also be used to restrict or potentially violate fundamental human rights such as freedom of expression or the right to privacy. This section outlines how ICTs enable the enjoyment of human rights and contribute to overall social and economic well-being. It also explores the human rights risks and challenges the sector faces.

5.1 Benefits

According to the International Telecommunications Union (ITU), an estimated 3,2 billion people are Internet users, with almost 7 billion mobile phone subscriptions worldwide.[5],[6] Telecoms investment is largely bypassing fixed-line (or "landline") services in many countries and focusing on mobile technology and mobile Internet access. This innovation has reduced the cost of Internet access and circumvented the need to build landlines, thus avoiding the problem in some countries of an erratic electricity supply, which prevents people from accessing the Internet via a desktop computer. In addition, smart phones are relatively cheap compared to a laptop or desktop computer and do not rely on a constant electricity supply.

This connectivity is the driver of fundamental change, empowering people and changing the way we learn and communicate. The Internet and digital communications are valuable tools in enabling economic and human development, as well as in strengthening human rights protections. This is acknowledged in reports by the ITU and UNESCO, which highlight the importance of broadband to realise the United Nations Sustainable Development Goals adopted in 2015.[7]

This section highlights six areas where greater access to telecom services may produce potential benefits in terms of realisation of human rights:

- Economic inclusion and jobs
- Access to health
- Access to education
- Reduced climate impact
- Peace, justice, safety and social inclusion
- Freedom of expression

5 World Bank, "World Development Report 2016 - Digital Dividends", at: http://www.worldbank.org/en/publication/wdr2016

6 ITU, "The World in 2014: ICT Facts and Figures". See: http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf

7 See: http://www.broadbandcommission.org/documents/working-groups/bb-wg-taskforce-report.pdf

5.1.1 Economic Inclusion and Jobs

There is a strong correlation between the growth of mobile and Internet penetration and gross domestic product (GDP). The McKinsey Global Institute estimates that the Internet alone accounted for 21% of aggregate growth in GDP across thirteen of the world's largest economies from 2006 to 2011, with 10% of that growth occurring for small to medium size enterprises (SMEs).[8] The ICT sector is viewed as a trigger for increasing productivity and competitiveness and as an opportunity to shape a level playing field, which supports more and better jobs.

The World Bank has conducted research on the link between broadband penetration, growth and employment showing an effect of increased growth of 0.24-1.5% with increased penetration of 10% while indirect job creation was increased by 1.5-4.5% for every direct job created.[9] And it is not only penetration that impacts GDP. Doubling the broadband speed for an economy reportedly increases GDP by 0.3%.[10] Enhanced use of digital solutions among governments, businesses and consumers may increase productivity. For example, across the Nordics and Baltics it might mean a 3.5% increase in productivity while creating up to an additional 470,000 jobs.[11]

The World Bank also reported that the ICT sector accounts for one-quarter of GDP growth in developing countries. In India, the growth of mobile applications and mobile commerce has created 7 million jobs.[12]

One of Africa's mobile innovation success stories has been the increasing use of mobile payments (now found in many parts of the world), which were first introduced by the telecoms operator Vodafone as M-Pesa and launched in Kenya in 2007 by Safaricom, an Associate company. Mobile money services enable mobile money transfers, bill and merchant payments, and savings using mobile devices. These services have a positive impact on people's ability to transact, pay, and save money, which in turn can support realisation of economic and social rights. It has transformed the ways of doing business, and enhanced financial inclusion, particularly for the large numbers of financially marginalised people who do not have access to formal bank accounts.

5.1.2 Access to Health[13]

Access to healthcare for patients in rural and remote areas is increased with m-health, e-health and telemedicine through for example training of health-workers, remote patient monitoring and information about healthy living. At an aggregated level, these services can

8 See: http://www.mckinsey.com/insights/high_tech_telecoms_internet/internet_matters

9 See: http://siteresources.worldbank.org/INFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/281747-1362494789452/2013-02-28_1330_2_Doyle_Gallagos_Broadband_Lightning_Talk.pdf

10 Ericsson. "New Study Quantifies the Impact of Broadband Speed on GDP." Press Release, 27 September 2011. See: http://www. ericsson.com/news/1550083

11 See: http://www.teliacompany.com/accelerating-sustainable-growth

12 Joshua Meltzer, Supporting the Internet as a Platform for International Trade: Opportunities for Small and Medium-Sized Enterprises and Developing Countries, Brookings Institution (Global Economy and Development Working Paper 69, February 2014). See: http://www.brookings.edu/~/media/research/files/papers/2014/02/internet%20international%20trade%20meltzer/02%20international%20trade%20version%202.pdf

13 ITU, UNESCO, "Transformative Solutions for 2015 and Beyond a Report of the Broadband Commission Task Force on Sustainable Development"

help prevent and manage diseases through for example early warning of disease outbreaks and provide real-time data collection. Digital health systems directly support efforts to increase access to health services and reduce human suffering from natural disasters and diseases.

5.1.3 Access to Education[14]

Distance and online courses increase access to and quality of education, regardless of location and level of development. ICT can facilitate teacher training and management information systems can increase efficiency and effectiveness of educational administrations. This is revolutionising opportunities of marginalised groups and creates potential for more inclusive societies where children and youth of different background are given similar opportunities to learn and develop.

5.1.4 Reduced Climate Impact[15]

ICT is an enabler of efficiency gains in energy generation, distribution and consumption in buildings, transportation, logistics and grids. The negative effects of climate change can also be reduced through, for example, providing resources for early warning systems for natural hazards. In many ways, ICT facilitates the transition from physical to virtual infrastructure decoupling economic growth from greenhouse gas emissions.

The understanding of environmental impact and development comes to a large extent from ICT systems of remote sensing, e.g. systems to track deforestation and Geographic Information Systems. Agriculture practices can be improved through smart agricultural practices, for example advisory over mobile phone push services. Likewise, ICT can improve water management and access to clean water. The link between climate change and human rights has been widely researched and established in recent years.[16],[17]

5.1.5 Peace, Justice, Safety and Social Inclusion[18]

A developed communications infrastructure can be key to the safety and security of citizens, in particular access to emergency services such as ambulance, police, fire and rescue. In times of national emergency, fully functioning communication systems are essential.

But ICT is also important to promote social inclusion and accessibility for persons with disabilities and other marginalised groups. In addition, public services and systems such as e-governance and e-voting are enabled and strengthened by ICT. Mobile services can also provide reporting and tracking on violence, harassment and corruption, which improves transparency and accountability in a society and ultimately strengthens the ability of citizens to exercise their rights.

14 Ibid
15 Ibid
16 See: http://www.ohchr.org/Documents/Issues/ClimateChange/COP21.pdf
17 See: http://apps.unep.org/publications/index.php?option=com_pub&task=download&file=011917_en
18 Ibid

5.1.6 Freedom of Expression

Freedom of expression is an enabling right, which means its enjoyment is essential in realising, promoting and protecting other human rights. As more people become connected through the use of ICTs, there are more avenues and platforms to seek, receive, and impart information, share ideas, raise awareness of issues, participate in governance at all levels and bring about positive change.

5.2 Challenges

ICT and broadband networks are intended to enable people to communicate. However, there is the potential for ICT to be used by governments and others in ways that may undermine the protection of human rights.

- One main challenge for the sector involves the complex, diverse or contradictory legal frameworks that a exist in countries around the world and the reality that no international normative framework currently exists to govern telecommunication companies in the context of human rights related issues. This poses challenges for the sector to act coherently and consistent with their responsibility to respect human rights as set out in the UN Guiding Principles.

- Another set of challenges emerges from the definition of "freedom online", which has reached international recognition.

5.2.1 Complex and Diverse Legal Frameworks

At the UN level, there have been various reports and resolutions that impact the telecommunications sector. In 2013, the UN General Assembly adopted a resolution on the right to privacy in the digital age[19], including a specific section on the role of business. The telecommunications sector is highly regulated (when compared to other elements of the ICT sector such as 'over the top' internet services) and the laws in different jurisdictions applicable to the sector are complex. For example, the domestic legal framework for legal interception differs from country to country, but at this time, there is no comprehensive source or database that gathers in one place all national laws related to aspects of the ICT sector, or telecom sub-sector, that can impact human rights. In some cases, national laws may conflict with international human rights standards and commitments – a point addressed specifically by Principle 23 of the UN Guiding Principles on Business and Human Rights and one which underpins most of the key dilemmas set out in this paper.

19 See: http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx

However, relevant information on such issues is gradually becoming available. For example, a Global Network Initiative (GNI) report, Opening the Lines[20], compared laws from the UK, Sweden and Russia, and demonstrated the variety and range of access and interception considered "lawful" in these countries. More recently, some telecom companies, such as Vodafone and Telenor, have started to include in their transparency reports descriptions of legal requirements around surveillance and monitoring, filtering and blocking of content, and network interruptions and shutdowns. These transparency reports are a useful source of legal information, though limited to countries in which the companies have operations. Adding to the work by Telenor and Vodafone, the Telecommunications Industry Dialogue (TID) has gathered and made available in a dedicated database under Creative Commons licenses, country legal framework information covering over 40 countries.[21]

An export control framework specifies the licensing requirement for products subject to export control, including those ICT products classified as "dual use".[22] This legal framework is in flux.[23] For example, the Wassenaar Arrangement[24] was recently expanded to include restrictions on the export of specific surveillance technology. This includes monitoring centres[25] and some aspects of "intrusion software[26]" but there is still debate as to how each Wassenaar member state will interpret these restrictions.[27]

As a result of this incomplete and emerging international legal framework governing ICT products and the conduct of ICT companies, the articulation of the legal or ethical responsibilities of network vendors and operators and those who are directly linked to them through business relationships is equally incomplete. The ICT sector therefore relies on the UN Guiding Principles, as well as other emerging concepts, such as "freedom online", good practices suggested by experts, and reflections of reported incidents in relation to telecom products and operator conduct, as signposts in clarifying the human rights due diligence expectations of telecom companies. Industry-specific standards have been developed by multi-stakeholder initiatives, industry associations, and other bodies which aim to develop more detailed guidance for ICT companies. This includes the GNI Principles and Implementation Guidelines,[28] as well as the TID Guiding Principles,[29] and other efforts including the European Commission's ICT sector guidance[30] for the corporate responsibility to respect human rights.

---

20 See: https://globalnetworkinitiative.org/sites/default/files/GNI_OpeningtheLines.pdf

21 See: http://www.telecomindustrydialogue.org/resources/country-legal-frameworks/

22 The definition for the Commission's proposed export control reform for dual-use items goes beyond telecoms; includes also electronics, semiconductor and computing industries.

23 For the European Commission's ongoing plans on export control reform, see: http://europa.eu/rapid/press-release_IP-16-3190_en.htm

24 The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual Use Technologies (the "Wassenaar Arrangement") produces two control lists: the list of Dual Use Goods and Technologies and the Munitions List. The Munitions List contains items designed for military use, including but not limited to items such as tanks and other military armed vehicles, combat vessels and aircraft. The List of Dual-Use Goods and Technologies contains several categories of goods that can both have a military and a civilian use, including electronics, computers, and telecommunications and information security equipment.

25 See: https://www.privacyinternational.org/?q=node/75

26 See: https://www.privacyinternational.org/?q=node/73

27 See: https://privacyinternational.org/?q=node/588

28 See: https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwixs8TGxfHRAhWhBcAKHUNnDOIQFggcMAA&url=https%3A%2F%2Fglobalnetworkinitiative.org%2Fimplementationguidelines%2Findex.php&usg=AFQjCNG7dvuqmJz1r1M0iEfwaRfV9AoA0w

29 See: http://www.telecomindustrydialogue.org/tag/tid-principles/

30 See: https://www.ihrb.org/focus-areas/information-communication-technology/report-ict-human-rights-sector-guide

5.2.2 Freedom Online

A resolution adopted at the 20th session of the UN Human Rights Council in 2012, titled "the Promotion, Protection and Enjoyment of Human Rights on the Internet"[31], affirmed that the same rights people have "offline" must be protected "online", including freedom of expression. Other resolutions have repeated this point.[32] Therefore, an assessment of repression "online and offline" should serve as an "umbrella principle" that guides assessment of freedom online.

The Freedom Online Coalition (FOC) was founded in 2011 as a partnership of governments (30 governments participating at the time of writing) working to advance Internet freedom. The Government of Sweden is a founding member of the initiative. The Freedom Online Coalition Joint Action for Free Expression on the Internet highlights areas of concern where governments are limiting online expression contrary to their duty to protect freedom of expression. It refers specifically to:

> *"Illicit monitoring, filtering and hacking, on- and offline repression of network technology users, including intimidation and arrests, and even completely shutting down the Internet and mobile networks."*[33]

The fourth Freedom Online Conference in 2014 adopted a set of Recommendations for Freedom Online also known as the Tallinn Agenda, which includes more specific commitments by FOC members.[34]

Reports by the previous UN Special Rapporteur on Freedom of Expression, Frank La Rue, featured the topic of freedom of expression on the Internet for the first time. These reports pointed to issues including:

> *"Arbitrary blocking and filtering of content, criminalisation of legitimate expression, imposition of intermediary liability, disconnecting users from internet access, including on the basis of intellectual property laws, cyberattacks and inadequate protections of the right to privacy and data protection."*[35]

Current UN Special Rapporteur David Kaye has also focused on the role the private sector with regard to freedom of expression online, and he is currently preparing a report that

31 See A/HRC/20/L.13 29th June 2012 The Promotion, Protection and Enjoyment of Human Rights on the Internet http://daccess-dds-ny.un.org/doc/UNDOC/LTD/G12/147/10/PDF/G1214710.pdf?OpenElement

32 See also UN Resolution A/RES/68/167 http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167

33 See: https://www.freedomonlinecoalition.com/wp-content/uploads/2014/04/1-The-Hague-FOC-Founding-Declaration-with-Signatories-as-of-2013.pdf

34 See: https://www.freedomonlinecoalition.com/wp-content/uploads/2014/04/FOC-recommendations-consensus.pdf

35 See, A/HRC/17/27 "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue: (27th May 2011), at; http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27.Add.1_EFSonly.pdf

is specifically focused on the role of the telecommunications and internet access sector.[36]

From these resources and initiatives, some common themes emerge when describing "freedom online", including freedom from:

- Monitoring/Surveillance
- Blocking and filtering of online content
- Network shutdowns

The table below maps some of the human rights risks associated with telecommunications, based on the description of "freedom online".

Human Rights Risks	Monitoring / Surveillance	Blocking / Filtering Content (censorship)	Network Shutdowns
Freedom of Expression	Surveillance of person's communications can limit the exchange of information and ideas resulting in a "chilling effect" on freedom of expression, as people are less likely to express themselves freely if they know they are being observed or monitored.	Internet censorship limits the exchange of information and ideas and can suppress discussion and debate.	Preventing access to or the exchange of information impacts the right to seek, receive and impart information.
Right to Privacy	The act of surveillance, whether physical or of a person's communications is an inherently intrusive act and risks violating a person's privacy.	Interfering with private communications by blocking certain keywords or changing content interferes with the right to privacy.	
Freedom of Association & Assembly	A person under arbitrary surveillance may be prevented from exercising this right, as they fear arrest for attending a protest or meeting, or fear endangering colleagues or sources.	Blocking information on certain protests or meetings can impact this right.	Shutting off communications can impact the ability for citizens to organise and mobilise action.

36 See: http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/OpinionIndex.aspx

Right to a Fair Trial	Surveillance of privileged communications, such as between a lawyer and client can impact on this right		
Right not to be Arbitrarily Arrested or Detained	Surveillance technology can be used to track and arrest political dissidents.		

Certain technologies, such as mass surveillance[37] technology and intrusion software[38] are examples of ICT technologies that have been linked to human rights abuses, including arbitrary surveillance, arbitrary arrest and even torture.[39],[40] With these tools, surveillance is not limited to those within a country's borders, which puts exiles or diaspora overseas at risk of intrusive surveillance.[41] For example, there is evidence that some governments use surveillance technology to target citizens residing overseas that may be critical of the government concerned.[42]

5.3 Responsibilities of the Network Vendor

The purpose of this section, as well as those which follow it, is to describe the nature of the human rights responsibility of different business actors.

37 In contrast to lawful interception, mass surveillance is understood to refer to the bulk access and/or collection of many users' communications without prior suspicion of individual targets. Therefore mass surveillance involves no individual target, no prior suspicion, is not time bound and due to the technology employed, potentially limitless. In contrast to technology provided for lawful interception, much of the technology for mass surveillance is unregulated. Taken from IHRB, "Human Rights Challenges for Telecommunications Vendors. Addressing the Possible Misuse of Telecommunications Systems. Case Study: Ericsson" (2014), at https://www.ihrb.org/focus-areas/information-communication-technology/report-digital-dangers-human-rights-challenges-telecommunications-vendors (p13). Also, see the problem definition in a blog published by the Freedom Online Coalition: https://www.freedomonlinecoalition.com/how-we-work/working-groups/working-group-2/direct-access-systems/

38 For the purpose of this paper the definition of intrusion software is is taken from the Wassenaar Arrangement, see: http://www.wassenaar.org/wp-content/uploads/2015/06/WA-LIST-13-1.pdf p. 209: Software specially designed or modified to avoid detection by 'monitoring tools', or to defeat protective countermeasures', of a computer or network capable device, and performing any of the following: a. The extraction of data or information, from a computer or network capable device, or the modification of system or user data; or b. The modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions.

39 See: https://www.fidh.org/International-Federation-for-Human-Rights/north-africa-middle-east/libya/16959-the-amesys-case-the-victims-anxious-to-see-tangible-progress

40 For the purpose of this paper the definition of intrusion software is is taken from the Wassenaar Arrangement, see: http://www.wassenaar.org/wp-content/uploads/2015/06/WA-LIST-13-1.pdf p. 209: Software specially designed or modified to avoid detection by 'monitoring tools', or to defeat protective countermeasures', of a computer or network capable device, and performing any of the following: a. The extraction of data or information, from a computer or network capable device, or the modification of system or user data; or b. The modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions.

41 See, TechUK, "Assessing Cybersecurity Export Risks" (November 2014), at: https://www.ihrb.org/focus-areas/information-communication-technology/report-human-rights-guidance-for-cyber-security-companies-techuk

42 Search for surveillance and human rights on: https://www.eff.org/cases/

A network vendor's responsibility is generally to prevent or mitigate the risk[43] of the telecommunications systems they provide from being misused, and to demonstrate their efforts in this regard. It is also the legal responsibility of the network vendor to ensure appropriate licenses are obtained for products subject to export control, including those classified as "dual use". Beyond this, vendors should perform due diligence on prospective customers aligned with the UN Guiding Principles.

The same capabilities built into telecommunication networks to increase communication or as part of cyber security[44] technology can enable surveillance or disrupt, deny or degrade online services. If used inappropriately by the end user, this can pose a risk to human rights.

To implement the UN Guiding Principles, network vendors should develop human rights policies and practices and put them into practice in a sales compliance system screening human rights risks associated with the destination country, operator, technology and intended use of technology. Network vendor responsibilities are discussed below with respect to three main human rights challenges.

5.3.1 Monitoring/Surveillance

A network vendor's responsibility is to prevent or reduce the risk of unintended use of lawful interception. In high-risk scenarios, a vendor may decide not to supply surveillance capability or consider mitigating actions.

As part of delivering telecommunications networks, operators are usually required under the national law of many jurisdictions to provide the technical means for an individual's communications to be intercepted for the purposes of assisting law enforcement in investigating and preventing crime, known as "lawful interception".[45] A network vendor would provide these systems for lawful interception for their customers, i.e. the operators. "An unintended use [of lawful interception] 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."[46]

This can pose a challenge for telecom vendors exporting this kind of technology. Legally mandated interception of communications may be for legitimate purposes, but may also be misused when government agencies place specific groups (such as political opposition parties, human rights defenders, ethnic, religious or sexual minorities) under arbitrary surveillance.[47]

43 Principle 13 of UN Guiding Principle on Business and Human Rights requires business to: "seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts."

44 Cyber security capabilities are most often intended to defend networks and protect people against criminal activity, such as bank fraud.

45 For example, providing the technical means for interception is a legal requirement for European companies under a 1995 Council of the European Union Resolution on law enforcement operational needs with respect to public telecommunication networks and services. See: http://cryptome.org/eu-intercept.htm

46 Ericsson, "ICT and Human Rights: An Ecosystem Approach" (2013), p14, at: http://www.ericsson.com/res/the-company/docs/corporate-responsibility/2012/human_rights0521_final_web.pdf

47 It should be noted that other vendors, such as specialised providers of surveillance technology, may supply these services to governments or operators independently of the network vendor. It should also be noted that telecoms vendors do not have to apply to licensing operating conditions like the operators, i.e. whether or not to supply this technology even to operators is a company decision for vendors, not a legal obligation.

5.3.2 Blocking/ Filtering Content

A network vendor's responsibility is to assess the risk of unintended use of blocking and filtering. In high-risk scenarios consider prevention, mitigating actions or not providing the technology.

Governments may require operators to install some kind of blocking/filtering software on a telecommunications network. This could be to prevent spam, block illegal content such as child abuse images and other sites such as gambling. The vendor must consider the likelihood that such technology may also be used for censorship, to block/filter independent news sites, social media etc.

5.3.3 Network Shutdowns

A network vendor's responsibility is to prevent or mitigate the risk of the telecommunications systems they provide from being misused, and to demonstrate their efforts in this regard. Vendors have limited possibilities to minimise the risk of network shutdowns. From a customer and financial perspective shutdowns are detrimental to both customer loyalty and revenues. The network vendor does not deal directly with issues involving third parties, such as requests to remove or block online content, government requests for user information, or requests to suspend networks, as operators regularly face.

5.4 Responsibilities of the Telecom Operator

A telecom operator's responsibility is in general to identify, assess, prevent and mitigate any adverse impact to human rights associated with their services.

The license requirement to provide telecommunications services is normally between the government of a country and the operator; therefore, there may be a legal obligation (when such laws are in place) to allow monitoring/surveillance, block or filter certain content, or respond to requests/orders to shutdown networks or suspend certain services. Below are some examples where operators have a responsibility to identify, assess, prevent and mitigate any adverse impact to human rights associated with their services.

5.4.1 Monitoring/Surveillance

In cases of government request for information about customers, a telecom operator´s responsibility is to interpret government demands from a freedom of expression point of view as narrowly as possible, seek clarification from the government with regard to the scope and legal foundation for such demands, require a court order or equivalent before meeting government requests for data, and communicate transparently with users about risks and compliance with government demands. In cases of intelligence agencies directly connected to the operator´s network, the operator should, if allowed, be transparent about such knowledge.

In Western Europe, the US and a number of other countries, authorised law enforcement agencies seeking to intercept content of communications must first seek court or political authorisation and present a warrant to the operator.[48] When a warrant is presented, the operator is obliged to provide interception and deliver or provide access to requested information.

In some countries, state intelligence agencies define interception procedures. In some cases, even when warrants may be required for interception, they are not required to be presented to any party, and operators cannot ask to see them.[49]

There are ongoing debates and discussions about the best way to provide interception procedures. In particular, the UN Resolution on the Right to Privacy in the Digital Age[50] states:

"Where enterprises are faced with government demands for access to data that do not comply with international human rights standards, they are expected to seek to honour the principles of human rights to the greatest extent possible, and to be able to demonstrate their on-going efforts to do so… There are positive examples of industry action in this regard, both by individual enterprises and through multi-stakeholder initiatives."

Intelligence Agency control centres are in some countries directly connected to the operator's network, enabling the intelligence agency to have direct access to communications.[51] This can leave operators in a difficult position when it comes to respecting human rights, such as privacy of their users.

5.4.2 Blocking / Filtering Content

A telecom operator´s responsibility is to restrict blocking and filtering demands by only catering to specific justifiable requests where infringement on freedom of expression is minimised.

When governments require operators to block particular content running over the network, it is the operator's responsibility to mitigate adverse impacts on human rights such as freedom of expression. For example, restricting access to certain pieces of content may be justifiable, but restricting access to entire websites or social media services or independent news sites is likely to infringe on freedom of expression, and there would be questions as to whether this was a proportionate action. Operators should seek ways to challenge such requests, while recognising that they may be legal in many national contexts.

48 IHRB notes that mass surveillance is increasingly becoming legal in many European countries. Court orders for targeted interception in those cases do not apply, nor do any other safeguarding mechanisms for ensuring necessity, proportionality or legality. See: https://www.ihrb.org/focus-areas/information-communication-technology/report-lawful-interception-and-government-access-to-user-data

49 Ibid, p. 12

50 UN Human Rights Council, "Right to Privacy in the Digital Age", A/HRC/27/37 30th June 2014 (para 45) http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

51 See: IHRB, "Human Rights Challenges for Telecommunications Vendors. Addressing the Possible Misuse of Telecommunications Systems. Case Study: Ericsson" (2014), at https://www.ihrb.org/focus-areas/information-communication-technology/report-digital-dangers-human-rights-challenges-telecommunications-vendors. The transparency report by Telia Company refers to laws on direct access throughout its geographies, pages 17-19. See: http://www.teliacompany.com/globalassets/telia-company/documents/about-telia-company/ledr_oct2016_final.pdf

5.4.3 Network Shutdowns

A telecom operator´s responsibility is to minimise time and scale of network shutdowns. Governments may require, by law, operators to shutdown certain services typically in times of "national emergency".[52] While laws governing network shutdowns are often vague, it is the responsibility of the operator to make best efforts to mitigate the risk to human rights in cases where the requests are not necessary or proportionate. For example, experts have stated that shutting down access to an entire country is difficult to justify under human rights law.[53]

Export Credits and Human Rights

6

This section begins by defining human rights responsibilities in export credit transactions in a broader sense. It then elaborates on how export credits could be regarded with reference to the three different types of potential business involvement in adverse human rights impacts as defined by UN Guiding Principles - "cause", "contribute" or "being linked to". This is followed by a number of proposed principles and main building blocks for an export credit human rights due diligence framework for telecom transactions.

6.1 Responsibilities

The responsibility of the export credit system is to review the exporter and in high human rights risk situations review the buyer's policies and practices with regard to human rights due diligence. If the Export Credit System is linked to adverse human rights impact they should explore ways to mitigate future adverse impact.

52 Some countries' legal frameworks give wider powers to governments with regards to service restriction.

53 Special Rapporteurs on freedom of expression from the United Nations (UN), the Organisation of Security and Co-operation in Europe (OSCE), the Organisation of American States (OAS) and the African Commission on Human and People's Rights, have all concluded that cutting off access to the internet can never be justified under human rights law, including on national security grounds. Joint Declaration on Freedom of Expression and the Internet (2011) Article 6b. http://www.osce.org/fom/78309?download=true
See also IHRB's Digital Dangers report: Corporate Responses to Network Shutdowns. Case Study: Telenor Pakistan http://www.ihrb.org/publications/reports/digital-dangers-case-study-pakistan.html

The UN Guiding Principles expect businesses to both "know and show" that they have done their due diligence and addressed human rights risks and impacts. In his remarks in 2010 to the OECD concerning export credit agencies and human rights, author of the UN Guiding Principles, former UN Special Representative John Ruggie stated that export credit agencies should conduct human rights due diligence themselves, and where ever their access allows require human rights due diligence of project sponsors.

According to the UN Guiding Principles, the responsibility to respect human rights requires that business enterprises:

- Avoid causing or contributing to adverse human rights impacts through their own activities, and address such impacts when they occur
- Seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts.

The UN Guiding Principles distinguish between the responsibility to "avoid" and the responsibility to "seek to prevent". In the commentaries to the UN Guiding Principles, it is noted that "activities" are understood as including both actions and omissions; and "business relationships" are understood to include relationships with business partners, entities in the value chain, and any other non-State or State entity directly linked to business operations, products and services. The UN Guiding Principles state that human rights due diligence:

"17. (a) should cover adverse human rights impacts that the business enterprise may cause or contribute to through its own activities, or which may be directly linked to its operations, products or services by its business relationships;"

A financial institution or an export credit agency could be considered to cause a human rights violation through its own activities by for instance, restricting trade unions or discriminating among clients on the basis of race and gender.[54] In the same manner, a financial institution could also be considered to contribute to a human rights violation through its own activities. In these cases a financial institution or export credit agency should "avoid" causing such adverse human rights impacts.

In a financial transaction, a financial institution or an export credit agency has the responsibility to "seek to prevent" or mitigate adverse human rights impacts that are directly linked to its product or service. This responsibility is more explicit in the case of export credits due to the connection to the state.

54 See OECD, "Scope and application of 'business relationships' in the financial sector under the OECD Guidelines for Multinational Enterprises" (2014), at: http://mneguidelines.oecd.org/globalforumonresponsiblebusinessconduct/GFRBC-2014-financial-sector-document-2.pdf. See also, OECD, "Due diligence in the financial sector: adverse impacts directly linked to financial sector operations, products or services by a business relationship" (2014), at: https://mne-guidelines.oecd.org/globalforumonresponsiblebusinessconduct/GFRBC-2014-financial-sector-document-1.pdf

Based on the reasoning above, it can be concluded that export credit institutions should require risk based human rights due diligence in export credit transactions. In providing export credit guarantees or financing to exporters or international banks, there is a direct linkage through business relationships and a prospective responsibility to mitigate any future adverse impacts. As the purpose of an export credit transaction is to support exporters, the Swedish export credit system normally has a direct business relationship with the network vendor and an indirect business relationship with the telecom operator.

6.2 Human Rights Due Diligence in Telecom Transactions

This section offers a proposed framework for human rights due diligence (HRDD) for export credit institutions when providing guarantees or financing in telecom transactions. The framework is specifically aimed at the exports of telecom vendors.

The framework is a risk based approach in line with the European Commission's ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights (The Guide).[55] The Guide outlines the framework for assessing, integrating, tracking and communicating human rights risks in general as set out in the UN Guiding Principles. Some key characteristics of the assessment phase of the framework are discussed below in the context of telecom transactions.

The European Commission Guide stresses the importance of identifying actual and potential impacts on people that might happen as a result of business activities or through business relations.[56] The broader operational context becomes important, including factors such as conflict, corruption and weak governance.[57]

A business must understand the presence of vulnerable groups in its specific context. These are groups within a society who may experience political, social or economic marginalisation that makes them particularly vulnerable to adverse impacts linked to business activities.[58] In the telecom sector, such groups may include opposition parties or minorities that are repressed by a non-democratic government.

It is important to assess the business relationship in a specific transaction[59] and the capacity of the network provider and operator to manage human rights risks. This includes factors like experience, track record and management capacities of telecom equipment vendors

55 European Commission, "ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights" (2013), at: https://www.ihrb.org/focus-areas/information-communication-technology/report-ict-human-rights-sector-guide
The Guide applies the UN Guiding Principles to the specific context of the ICT sector. Recognising that each company is different, it summarises what the UN Guiding Principles expect, offers a range of ideas and examples of how to put them into practice, and links the user to additional resources that can support their work. It is intended to help ICT companies "translate" respect for human rights into their own systems and cultures.

56 Ibid, Section 2: Assessing Human Rights Impacts pp27-41

57 Ibid p30-31

58 Ibid p38-39

59 Ibid pp32-36

and telecom operators to manage human rights risks.

The assessment of the business activity includes identifying activities commonly associated with adverse human rights impacts. In the case of telecoms this could be providing certain high-risk technology.

6.2.1 A Framework for Export Credits and Telecom Transactions

A due diligence process for export credits in telecom transactions could be based on key characteristics of the European Commission's ICT Sector Guide on Implementing the UN Guiding Principles and aligned with the lifecycle of an export credit transaction. The framework consists of four parts:

- Undertaking risk assessment of exporter and transaction
- Integrating findings in credit decision
- Tracking through monitoring and remedy
- Communicating and engaging

The Export Credit System's human rights due diligence should include an assessment of the following four core components of the concept of "freedom online":

- Respect for human rights both online and offline
- Monitoring/Surveillance
- Blocking and filtering of online content
- Network shutdowns

6.2.2 Risk Assessment of Exporters

The export credit system should include review of regular large customers' human rights due diligence process to verify that human rights risks are adequately reviewed in their internal risk systems. In the telecom sector, particular emphasis should be on the exporters' human rights due diligence process regarding:

- legal compliance
- country operational context
- operator characteristics
- technology for export

The quality of the exporter's due diligence documentation will have a significant impact on the efficacy of the Export Credit System's due diligence and influence the outcome of the Export Credit System's credit decision.

6. 2.3 Risk Assessment of the Transaction

Upon application by an exporter or bank for export guarantee or credit, the export credit system should conduct its own human rights due diligence on a proposed transaction. The due diligence is separate from that the exporter should carry out for its operations, and should focus on the export credit system role and responsibilities and business relationships.

The scope of the due diligence at the application stage should include consideration of the Place, Product, Purchaser and Purpose of the transaction. Purchaser policies and practices would in telecommunications transactions be the operator. Together, this makes an assessment of the "Four P's". As the application progresses, the export credit system and the exporter can work together on further mitigation strategies where necessary as more information on the human rights risks is obtained as part of continuing due diligence and confidential discussions.

The table below lists the main components of the risk assessment on a transaction level followed by comments on practical difficulties and high risk indicators.

Place	Country Risk Assessment
The human rights situation in a country should be assessed considering the "Freedom Online" framework to determine if a place is high risk. Such information is available on online.	Human rights risks both offline and online should be estimated, including: • Monitoring/Surveillance: Level of privacy/freedom of expression • Blocking/Filtering Content (censorship): Freedom of expression • Network Shutdowns: Freedom of expression, plus a host of human rights that are impacted during shutdowns such as assembly, health, education, work. Non-democratic governments or democratic governments with a strong military influence are considered high risk and so is presence of severe conflict, political turmoil, weak governance and corruption
Product	**Technology Risk Assessment**
It is the responsibility of the export credit system to ascertain that the exporter has carried out the relevant legal reviews and all relevant export licenses are in place.	The applicant/exporter's own assessment of the products should clarify the following aspects for the export credit system: • The exporter's legal compliance with all appropriate export controls. • A general estimation of technology related human rights risk of the exported technology. • A general assessment of the exporter's ability to manage technology related human rights risks including mitigation of unintended use of the technology.

Purchaser	Operator Risk Assessment
The operator has a responsibility to mitigate adverse impacts to human rights.	Ownership structure: State owned operators are generally closer to their government than private operators or operators owned by foreign parent companies. Operator policies to respect human rights both offline and online: These policies should include handling of general human rights risks mentioned earlier in this paper. The existence of policies in these areas would demonstrate the operator's willingness to mitigate risks to human rights and to operate independently of the State. Operator Practices: If an operator has previously been involved in any incidents that impact negatively on human rights, how they acted to mitigate/resolve the issue and what additional policies (if any) were put in place or lessons learned.Examples of high risk operator characteristics are state-owned, lack policies and practices or have been involved in previous human rights related incidents.

In a country risk assessment it is often difficult to find what laws are relevant to telecommunications companies in a country. However the country risk assessment process is supported by knowledge about the application of a country's legal framework, including analysis of national laws that provide more or less human rights protection than internationally recognised human rights, or conflict with internationally recognised human rights standards, and how they are enforced.

In the technology risk assessment, confidentiality may restrict exporters to share information. Due to product security and technological confidentiality, it is recognised that the export credit system is restrained in the extent to which it could achieve detailed information on a product level. The export credit system has to rely on the applicant/exporter's own risk assessment of the products.

6.2.4 Integrating Findings in Credit Decisions

In a low risk scenario, the export credit system would rely on the institutional capacity of the export destination country as well as its review of the exporters' sales compliance process to verify that human rights risks are adequately reviewed and managed.

In such a risk scenario further actions are not required and the export credit system could proceed with the transaction from a human rights perspective with the condition that relevant export licenses are in place.

A high-risk scenario is identified as a combination of factors. These factors relate to the Place, Products, Purchaser and Purpose. The magnitude of the overall risk factors should trigger an internal discussion about the best way to proceed with the transaction, whether risk mitigation is possible and if so how, and further consultation with the exporter, leading to a management decision. Such decision may include a decision:

- to proceed with the transaction;
- to proceed with mitigating action;
- not to proceed with the transaction; or
- to escalate the approval process to the company board.

It is suggested that a transaction involving a high risk country, combined with a high risk product (technology) without any risk mitigation, and a high risk operator without any risk mitigation and without a clear low risk purpose should lead to a decision to escalate the approval process and could also lead to a decision not to support the export.

If a Place is deemed high-risk, the export credit system has little leverage to change conditions in country. However, there could be opportunities to mitigate risks to human rights by:

- Taking advantage of existing dialogue in diplomatic bilateral relationships through embassies or the Ministry of Foreign Affairs (MFA) or;
- Asking the Ministry of Foreign Affairs to open dialogue to facilitate discussion of the human rights issues in the ICT sector.

The decision to proceed in high risk scenarios would be based on further assessment of the Product and Purchaser, where there may be some leverage to mitigate risks to human rights.

In the event of a high risk Product to a high risk place or purchaser, the export credit agency could check that the exporter has considered reducing the product risk level as well as other risk mitigating actions not directly related to the technology (see below).

If a Purchaser is deemed high risk, the Export Credit System has some leverage. EKN and SEK have in some cases been able to visit the operators and ask further questions about their policies and suggest improvements. The export credit system could also work with the exporter and bank to put in place relevant mitigating actions regarding training, user statements, usage etc.[60]

6.2.5 Tracking through Monitoring and Remedy

Risks to human rights may arise at a later date because: the situation in the country changes (as happened recently in Ukraine where the security situation changed very quickly); personnel changes at government ministries may bring a different point of view about security; or the product or service is found to have been misused. Regular follow-up of high risk transactions, could in some cases help uncover misuse of the product and allow the export credit system to take steps to prevent future adverse impact. To be able to receive confidential information about adverse human rights impacts and other misconduct in companies with which the export credit system has a business relationship,

60 Institute for Human Rights and Business, "Digital Dangers: Human Rights Challenges for Telecommunications Vendors: Addressing the Possible Misuse of Telecommunications Systems Case Study: Ericsson" (2014), at: https://www.ihrb.org/focus-areas/information-communication-technology/report-digital-dangers-human-rights-challenges-telecommunications-vendors

it is relevant to have whistle-blowing mechanisms in place.

Finally, assistance of the respective boards at EKN and SEK, as well as consultation with the Ministry of Foreign Affairs following confidentiality laws and regulations could be undertaken when a high risk country is involved (whether determined as high risk at the outset of the transaction or later when conditions change). Developments in the host country should be recorded and shared with the relevant teams within the export credit agency to ensure coherence of operational policies.

Notwithstanding thorough due diligence, human rights harm can occur in the host country, post-export, when the export credit agency will have no leverage or means to remedy such harm. In view of the fact that the export credit agencies will have no contractual relationship with the operator directly, it will be difficult for the export credit agency to insist that the operator remedy human rights harm that occurs through operator acts or omissions. However, the Export Credit System may be able to use its position to play a role in encouraging an operational level grievance mechanism at the operator's level.

It should be noted that the Export Credit System itself will be subject to the OECD National Contact Point procedure in the event of a complaint under the OECD Guidelines on Multinational Enterprises.

6.2.6 Communicating and Engaging

Communication and transparency is an important foundation of the UN Guiding Principles. The transparency of the Swedish Export Credit System is bound by laws and regulations governing public information and commercial secrecy as well as bank secrecy. Within these boundaries EKN and SEK has defined in dialogue with stakeholders what a possible level of transparency is for the respective organisations. This includes publication of summary due diligence of high risk situations in their respective Annual Reports.

Regardless of legal leverage, the Export Credit System has the responsibility to engage with all the relevant parties within the transaction to encourage them to fulfil their responsibility to respect human rights. Such engagement may occur with the following parties:

- **The exporter:** The exporter has a direct business and legal relationship with the operator and should have some leverage on the purchaser. The exporter could be encouraged to seek further engagement with the operator. However, this should ideally be part of the Export Credit System's due diligence of the Exporter's human rights due diligence procedures and not a case-by-case event.

- **The bank:** The bank has a direct business relationship with the operator and can encourage the operator to minimise human rights risks. As an early mover, the Swedish Export Credit system can take the opportunity to engage with international banks to discuss practical ways of addressing human rights risks in the telecom sector.

- **The operator:** In high-risk scenarios, the Export Credit System may in some cases have already chosen to engage with the operator to understand their due diligence

process. In situations where something has gone wrong, the Export Credit System may choose to use existing relationships to encourage the operator and/or other involved parties to put in place policies and practices to prevent a repeat of harm.

- **Host government:** Due to the position of providing business finance, the Export Credit System might in very rare circumstances be able to engage high-ranking government officials. They also have the possibility to involve officials from the Ministry of Foreign Affairs and embassies, as already noted.

7 Final Remarks

The human rights issues associated with the ICT sector are very complex and are only recently receiving full attention from companies and business and human rights practitioners alike. The human rights due diligence methodology for this sector undoubtedly will evolve over the next few years, as the nature of human rights violations that could accompany the sector becomes better known and anticipated. Technology itself will evolve and this might present new solutions for current dilemmas but also present new human rights risks. IHRB commends EKN and SEK for initiating the discussion on what constitutes "freedom online" and the scope of their due diligence when they support Swedish telecommunications exporters.

This paper should be helpful in explaining to all the relevant stakeholder groups the role and responsibilities of the Swedish Export Credit System in financing telecom transactions. It is expected to improve the internal procedures for human rights due diligence in the Swedish Export Credit System.

Appendix: Applying Current Standards to the ICT Sector

A

	Provisions relevant for finance, and more specifically export/trade finance	Required due diligence scope, process for export/ trade finance	Remediation and Other observations
UN Guiding Principles on Business and Human Rights (UN GPs)	Although the UN Guiding Principles apply to all sectors, they are not specific about how they apply to different financing structures; in particular, how the classification of "causing" or "contributing to" adverse human rights impacts (in each case through the financial institution's own actions or omissions), or being "directly linked to" adverse impacts (through business relationships) should be applied to different financing structures is not explicit.	Guiding Principle 4: "*States should take additional steps to protect against human rights abuses by business enterprises that are owned or controlled by the State, or that receive substantial support and services from State agencies such as export credit agencies and official investment insurance or guarantee agencies, including, where appropriate, by requiring human rights due diligence.*" While due diligence is required in principle, the scope of it for export or trade finance is not explicit. The European Commission has published an ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights. While it is not yet certain that such a Guide achieved a stature of internationally recognised standards, in the event that the export credit agency decides to refer to it, there are specific useful due diligence steps.	In the case of "causing," or "contributing to" adverse human rights impacts, the company/financial institution should remediate, or contribute to the remediation of the impacts, respectively. In the case of adverse impacts through business relationships, the company/ financial institution has a forward-looking responsibility to avoid or mitigate the impact.

OECD MNE Guidelines applied to financial sector	Export and trade finance scenarios are likely to be either "contributing to" adverse impacts through the financial institution's own actions or omissions, or "directly linked to" adverse impacts through business relationships. These two concepts are "along a spectrum and it is likely that in some circumstances there will not always be clear answer."	Due diligence of the underlying business that will benefit from the transaction, and, in the case of direct linkage through business relationship, the business partners will be part of the due diligence process.	Same as above.
OECD Common Approaches	In the case of project or corporate finance for a specific project, the Common Approaches point to the IFC Performance Standards.	The focus of due diligence will be on the physical environmental and social impacts. Unless a large-scale physical installation is intended, the project will likely be categorised as C (and in rare cases, B).	Category C projects are not likely to specify any remedial actions.
IFC Performance Standards	In the case of project finance or corporate finance for a specific project, and in certain high-risk cases involving financial intermediaries, the Performance Standards apply.	While the circumstances under which IFC will require a specific human rights due diligence is not made public, the absence of significant physical footprint on the ground in most ICT sector projects or transactions means that this requirement will not be invoked. The due diligence focus will be on the physical environmental and social impacts. Unless a large-scale physical installation is intended, the project will likely be categorised as C (and in rare cases, B).	Category C projects are not likely to specify any remedial actions.