© Photo: ILO/Asrian Mirza

Part 2

Human Rights and the ICT Sector

Human Rights and the ICT Sector

2

Human Rights Impacts in the ICT Sector

Human rights are basic standards aimed at securing dignity and equality for all. Every human being is entitled to enjoy them without discrimination. They include the rights contained in the "International Bill of Human Rights" – meaning the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights. Those documents set out a range of rights and freedoms such as the rights to life, to freedom of expression, to privacy, to education, and to favourable conditions of work, to name a few. Internationally-recognised human rights also include the principles concerning fundamental rights set out in the International Labour Organisation's (ILO) Declaration on Fundamental Principles and Rights at Work, which addresses freedom of association and collective bargaining, forced labour, child labour and non-discrimination. In addition, some potentially vulnerable or marginalised individuals and groups are the subject of international human rights instruments that help provide clarity on how human rights apply to them (for more on this, see Section II-A). (See Annex 1 for a list of relevant instruments.)

Responsible ICT companies have become increasingly active in recent years in understanding and addressing the range of human rights issues linked to their products, services or technologies. They recognise that they can both positively and negatively impact their staff, workers in their supply chain, customers, users or the communities around their operations.

The ICT sector has come to play an important role in promoting human rights. For example, mobile banking and remote access to learning and to medical reports have all contributed to the reduction of poverty and improvement of health, education and livelihoods; new location technologies have helped save lives in the aftermath of natural disasters; and the development of the online environment and of social media have contributed to democratic movements and the enjoyment of freedom of expression worldwide. Even relatively small ICT companies can have global reach and significant human rights impacts.

Those ICT companies that are able to understand and manage a relatively complex set of business and government relationships, even with comparatively small resources, will be well-placed to build and maintain a high degree of stakeholder trust and accountability. On the other hand, those ICT companies that do not pay enough attention to human rights will run increasing risks of serious negative impacts resulting in worker, customer or user dissatisfaction, possible lawsuits and reputational harm.

Some ICT companies have come together to launch initiatives aimed at developing tools and supporting good practice with regard to respect for particular human rights in the sector, including the multi-stakeholder Global Network Initiative (GNI), which now houses the Telecommunications' Industry Dialogue on Freedom of Expression and Privacy, and the industry-led Electronic Industry Citizenship Coalition (EICC) and Global e-Sustainability Initiative (GeSI). There has also been active business involvement in a number of government-led initiatives, such as the Stockholm Internet Forum (see Enhancing Internet Freedom and Human Rights Through Responsible Business Practices) and the "Freedom Online" coalition.

Understanding the ICT Sector in this Guide

The ICT sector is best described as a complex "ecosystem", with actors ranging from telecommunications services providers to large equipment manufacturers to small software or Web-based start-ups. Individual companies in the sector may also play multiple roles – for example, manufacturing mobile phones and network components, or providing both mobile telecommunications and Internet access services.

For the purposes of this Guide, the following general terms are employed in describing different segments within the sector:

ICT Sector Segment	Description
Telecommunications services	Includes companies that provide: ▸ Fixed line and mobile telecommunications services (including voice and data); ▸ Consumer-facing wireless and Internet Service Provider (ISP) services; ▸ Internet "backbone" services; ▸ Network management services; ▸ Call centres to support these other services.
Web-based (and cloud-based) services/platforms	Includes companies that provide services/platforms for consumers and business end-users, including for: ▸ Search; ▸ Social networking; ▸ Cloud computing; ▸ Other "Web 2.0" services.
Manufacture of consumer and business end-user devices ("device manufacturers")	Includes companies that manufacture or sell (retail or wholesale): ▸ Cell phones and other mobile devices for accessing voice and data services; ▸ Computers and related equipment (e.g., printers); ▸ Consumer electronics equipment (such as televisions, gaming consoles, digital cameras).
Manufacture of telecommunications components, device components and network equipment ("component manufacturers")	Includes companies that manufacture or sell: ▸ Electronic components (such as semiconductors and chips) for consumer and business end-user devices; ▸ Passive (such as cell phone masts) and active (such as switches and routers) telecommunications network equipment.
Software	Includes companies that design, sell or distribute software that is: ▸ Physically packaged; ▸ Digitally downloaded; ▸ Pre-installed on computers, or other networked devices.

These general terms draw on the OECD's Guide to Measuring the Information Society and BSR's Protecting Human Rights in the Digital Age. Annex 2 contains further description of technical terms used.

Operating Contexts and the Relevance of the State Duty to Protect

The extent to which ICT companies may be involved with negative human rights impacts will be heavily influenced by both their operating context and the practices of their business partners. Both factors will shape the policies, processes and practices they need in order to prevent and address such impacts.

When states fail to meet their duty to protect, the responsibility of ICT companies to respect human rights does not change; however, it can become all the more challenging for them to meet that responsibility in practice. Areas in which state action (or inaction) can cause particular challenges for ICT companies include:

Responding to the fast pace of change: Many of the sector's products, services and technologies can have significant positive impacts on human rights; but if they are misused, they can also have negative impacts. Such technologies often develop much faster than regulators can react to their potential for negative consequences – for example, export control restrictions may lag behind technological developments and miss new products or new uses of existing products.

Protecting rights to privacy and freedom of expression: These rights can be particularly impacted by the operations of companies in the ICT sector. Under international human rights law, individuals' privacy or freedom of expression may be subjected to certain restrictions by governments (see Articles 17 and 19 of the International Covenant on Civil and Political Rights and Articles 12 and 19 of the Universal Declaration of Human Rights). Telecommunications and Web-based services companies can operate in domestic legal contexts where restrictions are not in line with international human rights law and/or where the state fails to protect these rights; yet in all cases, companies need to meet their own responsibility to respect in line with internationally-recognised human rights.

Government requests to ICT companies: Governments may make a range of requests that ICT companies provide information about customers and users for legitimate law enforcement purposes, block particular content or access to telecommunications or Web-based services, or tailor certain technologies to meet their specifications. These requests can be critical to a state's ability to meet its duty to protect human rights. However, where such requests are illegal (in that they do not have a basis in national law) or are not in line with international human rights law – for example, because they facilitate surveillance in order to persecute human rights defenders – this poses a direct challenge to an ICT company's ability to meet its responsibility to respect. The challenge may be acute for companies that are required to sign licensing agreements with a host state government in order to operate. Where a company has country operations, a government "request" may be accompanied by the intimidation of staff on the ground, making the appropriate response even more complex. Companies may be put in a position of potential contribution to (or complicity in) government abuses of individuals' human rights.

Absent, weak or poorly enforced labour laws: This can be relevant to all types of ICT companies with respect to their own workers. It can be particularly relevant to ICT companies with extensive supply chains (such as component and device manufacturers), since a significant amount of production in the sector takes place in domestic contexts that pose challenges in this regard. Where laws exist, but are weak or unenforced in practice, this can create a false sense of security for companies that the government is "doing its job". It may pose a particular problem where operations or suppliers are located in Export Processing Zones ("EPZs"), in which increasing amounts of ICT device and component manufacturing occur. Companies in EPZs may be exempted not just from certain taxes but also from various labour laws, for instance with regard to rights to form and join trade unions and collective bargaining. Even where such exemptions do not apply, it may be impossible for legitimate trade unions to gain access to workers in EPZs.

In situations such as these, merely obeying domestic laws is unlikely to be sufficient to demonstrate respect for human rights. Companies will typically need to do further, enhanced human rights due diligence to meet the increased challenges, as will be discussed in Part 3 of the Guide

Business Relationships

ICT infrastructure has historically been state-owned in many countries. While significant deregulation has occurred in the sector, private telecommunications services companies are often required to partner with state companies to deliver services, or increase service coverage. Even where this is not the case, private companies are required to obtain operating licenses from relevant national regulators.

In contrast, Web-based services companies use telecommunications infrastructure and networks to deliver their services but typically do not need to have a physical presence in the markets where they operate (though they may sometimes seek, or be required, to locate servers there). They also generally do not have a contractual relationship with the providers of the telecommunications services that they rely on. However, they can be subject to government requests when they operate in particular jurisdictions, just as telecommunications services companies may be, and some may also enter into agreements with governments.

End-user devices are typically made up of a large number of components so equipment manufacturers and telecommunications services companies can have extremely complex supply chains. Device manufacturing may be carried out by brand name "original electronics manufacturers" ("OEMs") or by "contract manufacturers", who

assemble and sell the finished device to a brand name OEM. Up to 80% of global ICT production has been outsourced by OEMs to five contract manufacturers, each employing tens of thousands of employees. OEMs that buy from the "big five" may stipulate which component suppliers the contract manufacturer can work with and/or directly source components that are then assembled by the contract manufacturer. OEMs may sell directly to business or individual end-users, or they may sell the equipment on to a telecommunications company that markets it under its own brand. Recycling of devices is usually contracted out to third parties.

Software companies may sell or distribute products directly to individual, business (including other ICT companies) or government customers, or via third party vendors, sometimes recruited on an incentive basis. Telecommunications services companies also make use of resellers and distributors in their sales processes.

All businesses in the ICT sector – whether suppliers, OEMs, resellers/distributors, or business customers or users – have their own responsibility to respect human rights, and this Guide is equally relevant to all of them. However, in some cases, companies may lack the awareness or capacity to meet the responsibility in practice; this poses risks to other ICT companies that are relying on them, as will be discussed in Part 3 of the Guide.

Understanding Potential Negative Impacts

While this Guide acknowledges the range of positive impacts that the ICT sector can have on human rights, respecting rights – that is, the avoidance of harm to human rights – is the baseline expectation of all companies. The Guide therefore focuses on the prevention, mitigation and remediation of negative human rights impacts.

The following matrix provides examples of the kinds of negative impacts that ICT companies may have. It is not intended to imply that every company will have these impacts, nor does it represent the full range of potential impacts of an activity. Rather, it is illustrative of the kinds of impacts that may arise and the rights that may be involved.

The matrix is structured in the following way:

- On the vertical axis, it lists a number of typical activities of ICT companies;
- On the horizontal axis, it lists some of the key stakeholder groups that different ICT activities may impact upon;
- In each box it gives an example of an impact that the particular activity may sometimes have on the stakeholder group, and the human rights that can be affected.

The matrix aims to show that:

- Different types of activities can have quite distinct impacts on different human rights;
- Negative impacts can happen throughout the life cycle of a product, service or technology;
- Different kinds of negative impacts can fall on different groups, and even on individuals within certain groups. Impacts can be more severe where individuals or groups are vulnerable or marginalised.

Analytical Framework for Assessing Potential Impacts of Company Activities on Stakeholder Groups

	Company Workers	Supply Chain Workers	Consumers and Users	Local Communities	Potentially Vulnerable or Marginalised Groups	Other Relevant Groups... (e.g., content creators)
Sourcing/ Value Chain Management	E.g., Security providers at a production facility abuse or threaten company workers with physical violence – *Right to Life, Liberty and Security of the Person*	E.g., Workers in mines producing minerals for ICT products are subject to forced labour and threats of physical violence - *Freedom from all forms of Forced or Compulsory Labour, Right to Life, Liberty and Security of the Person*	*Need to scan for emerging/one-off issues*	E.g., Inappropriate disposal of e-waste causes land/water contamination, leading to significant negative impacts on local community members' health and livelihoods - *Right to the Highest Attainable Standard of Health, Right to an Adequate Standard of Living*	E.g., Child labour used in extraction of minerals and/or informal recycling of e-waste – *Children's rights, including Freedom from Child Labour*	
Device Manufacturing	E.g., Local management inhibits workers' ability to freely join trade unions and refuses to engage in voluntary good faith collective bargaining – *Right to Form and Join Trade Unions, Right to Collective Bargaining*	E.g., Supplier factory located in unsafe area changes its shift times, requiring women workers to arrive/leave outside of daylight hours and exposing them to risks of attack – *Right to Life, Liberty and Security of the Person, Women's rights*	E.g., Government requires pre-installation of software onto devices (such as phones, laptops) that restricts access to "political" content or allows state surveillance that is not in line with international human rights law – *Right to Privacy, Freedom of Expression*	E.g., Factory releases toxic fumes that are not adequately treated or pollutes water resources that local community relies on leading to significant negative impacts on local community members' health and livelihoods – *Right to Highest Attainable Standard of Health, Right to Adequate Standard of Living*	E.g., Employment and recruitment agencies supplying workers to facilities take away migrant workers' passports once in-country and/ or subject them to high recruitment fees, leading to bonded labour – *Rights of migrant workers, including Freedom from all forms of Forced or Compulsory Labour*	
Component and Network Equipment Manufacturing	E.g., Student workers are required to work overtime and have their pay withheld by their school /college – *Right to Just and Favourable Conditions of Work, Freedom from all forms of Forced or Compulsory Labour*	E.g., Supplier factory workers lack adequate protective equipment and training, leading to significant negative impacts on their health – *Right to Highest Attainable Standard of Health*	E.g., Government demands URL filtering and blocking systems at the national network gateway for purposes that are not in line with international human rights law (e.g., to enable censorship of and limit peaceful public gatherings by human rights defenders) – *Right to Privacy, Freedom of Expression, Freedom of Assembly*	E.g., Land acquisition process for installation of network infrastructure does not allow meaningful consultation with local communities and results in inadequate compensation, leading to significant negative impacts on their livelihoods – *Right to an Adequate Standard of Living*	E.g., Cell towers and base stations are constructed on places of cultural heritage belonging to indigenous peoples, negatively affecting their ability to enjoy their sacred sites – *Rights of Indigenous Peoples, including to Self-Determination and Cultural Property Rights*	
Network Management	E.g., Staff are required to work excessive hours under conditions of high stress, leading to negative impacts on their health – *Right to Highest Attainable Standard of Health, Right to Just and Favourable Conditions of Work*	*Need to scan for emerging/one-off issues*	E.g., Host government license agreement requires a company to install network management software to collect and share personal information with the government for purposes that are not in line with international human rights law (e.g., to enable surveillance in order to persecute human rights defenders) – *Right to Privacy, Freedom of Expression, and if physical harm ensues, potentially other rights such as Freedom from Torture and Cruel, Inhuman or Degrading Treatment*	E.g., Server farms consume large amounts of energy, requiring complex cooling systems that use large amounts of water, negatively impacting on local communities' access to water – *Right to Highest Attainable Standard of Health, Right to Safe Drinking Water and Sanitation*	E.g., Discrimination against disabled workers in hiring process and failure to make reasonable accommodations in the workplace – *Rights of persons with disabilities, Non-Discrimination*	

	Company Workers	Supply Chain Workers	Consumers and Users	Local Communities	Potentially Vulnerable or Marginalised Groups	Other Relevant Groups... (e.g., content creators)
Management of Connectivity/ access	E.g., Staff on the ground are threatened by government officials when the government orders suspension of the telecommunications network during an election and staff resist because the request is illegal or not in line with international human rights law – *Right to Life, Liberty and Security of the Person*	E.g., Call centre workers are employed by contractors on renewable temporary contracts deliberately to avoid employment status and associated payment of wages and benefits under national law – *Right to Just and Favourable Conditions of Work*	E.g., A Web-based services company removes content that is not illegal because it does not have adequate review mechanisms in place – *Right to Privacy, Freedom of Expression*	*Need to scan for emerging/one-off issues*	E.g., Government requests users' personal information to target members of a particular racial or ethnic minority group for severe harassment or arbitrary detention – *Non-Discrimination, Rights to Life, Liberty and Security of the Person*	
Design and Engineering	E.g., Full-time and/or agency workers are denied the opportunity to join a legitimate trade union – *Right to Form and Join Trade Unions*	E.g., Small software company outsources its customer service function to a supplier that requires its staff to work excessive amounts of overtime – *Right to Just and Favourable Conditions of Work*	E.g., Failure to inform users of security breaches or to design appropriate updates results in human rights defenders being targeted with "malware" that infects their computers and prevents effective use – *Right to Privacy, Freedom of Expression*	*Need to scan for emerging/one-off issues*	E.g., Failure to build appropriate protections into websites or software typically used by, or targeting, children leads to children being harassed by other users and put at risk of abuse – *Children's rights, including Right to Privacy*	
Other Relevant Activities						