

ICT Sector Discussion Paper for Public Comment

Produced by The Institute for Human Rights and Business (IHRB) & Shift, 24 May 2012

NOTICE: Public Posting of all Written Comments

Unless expressly requested otherwise, submission of written feedback will be posted on the Project's web portal (<http://www.ihrb.org/project/eu-sector-guidance/index.html>) with each commentator's submitted name and organisational affiliation.

Key Questions for Written Comments

The [Project Team](#) welcomes written comments by all interested stakeholders on the following questions in particular. Please send comments to sectorguidance@ihrb.org by **30 June 2012**. ☒

- Does the discussion paper identify the most serious and the most likely impacts that companies in this sector may have on human rights?
- Does the discussion paper identify the major challenges that companies in this sector are facing in respecting human rights?
- Are there good practices in addressing these human rights challenges that could be built on in developing the forthcoming guide on the corporate responsibility to respect in this sector?
- What form should the forthcoming guidance take in order to add greatest value in advancing respect for human rights in this sector?

1. INTRODUCTION

This discussion paper is intended to help frame and stimulate discussion around key issues, challenges and opportunities regarding the implementation of the corporate responsibility to respect human rights under the [UN Guiding Principles on Business and Human Rights](#) (the UN Guiding Principles) in the Information and Communication Technology (ICT) sector.

Three important points concerning the scope of the project should be noted. First, in line with the UN Guiding Principles, the focus is on ensuring that businesses respect human rights – that they take action to avoid infringing on human rights and address any adverse impacts with which they are involved. This discussion paper therefore starts by identifying the most likely and/or most severe negative impacts that businesses in ICT sector may have on human rights. This in no way implies that all businesses have or will have these negative impacts, nor does it imply that businesses can have only negative impacts on human rights – it is well recognised that businesses can play a significant role in supporting human rights. However, respecting rights is the baseline expectation of all companies under the corporate responsibility to respect and accordingly that is the focus of this paper and sector guidance project.

Second, the corporate responsibility to respect is only one of the three pillars in the UN “Protect, Respect and Remedy” Framework and the Guiding Principles that implement it. The Guiding Principles recognise states’ existing obligations to respect, protect and fulfill human rights and fundamental freedoms and seek to elaborate on the policy implications of these obligations for states (referred to as the state duty to protect or first pillar of the Framework). This includes regulating corporate actions where appropriate. The UN Guiding Principles also recognise the need for appropriate and effective remedies for victims when their rights are

violated (the third pillar on access to effective remedy). While this project is focused on the corporate responsibility to respect human rights (the second pillar), the guidance will seek to take into account the various implications of the state's role in business' efforts to meet their corporate responsibility to respect, as well as businesses' responsibilities in access to remedies (third pillar). Nothing in this paper is intended to detract from the interconnected nature of the three pillars of the UN Framework.

Third, while the final guidance will take particular account of the situation and experiences of EU business, it aims to be as globally relevant as possible – informed by research and the views of a wide range of stakeholders, including representatives from business, civil society, trade union, and government, and experts – in order to contribute to a harmonised approach to the implementation of the UN Guiding Principles.

Please see [Annex A](#) for more background on the project, its timeline, and the UN Guiding Principles.

1.1 The Research and Consultation Process

This paper outlines the emerging issues arising from early-stage interviews with stakeholders representing business, industry association, trade union, civil society and expert perspectives, as well as input from individual members of the ICT [Sector Advisory Group](#) and European Commission [Expert Advisory Committee](#). However, this input does not constitute an endorsement of the views summarised in this paper by any individual member of the these advisory groups, or their organisations. Nor does this paper represent fixed conclusions on the part of the Shift and IHRB Project Team, but instead highlights a number of key emerging issues for further exploration and enquiry as part of the ongoing research and analysis process. Further stakeholder interviews will be conducted after the ICT sector roundtable in Brussels on 31 May 2012. In addition, the discussion paper will be posted for public comments on the project web portalⁱ and accepted up until June 30.

2. DEFINING THE SECTOR

The term information and communication technologies (ICT) sector is an expanded form of the information technology (IT) sector, applying scientific and engineering innovation for practical purposes (e.g. creating, storing, processing, and transmitting information), with the process of communication increasingly forming an integral part of the sector. The sector includes *products and their components* for information processing and communication (including transmission and display) using electronic processing to detect, measure, record and control physical processes.ⁱⁱ This includes products ranging from mobile telecommunication equipmentⁱⁱⁱ, hardware computing equipment of all types^{iv}, cabling, transmission towers and masts^v and other telecommunication infrastructure^{vi}, and processing equipment^{vii}. The sector also includes *services* intended to enable the function of information processing and communication electronically. This includes service companies ranging from those providing access to networks^{viii}, securing data in the electronic space^{ix}, providing space for users to create^x and share^{xi} data, images, and other files, providing the software architecture^{xii} to navigate the world wide web and means^{xiii} with which users can search for information on the Internet, and providing the software and operating systems running these various products themselves^{xiv}. The telephone, cable, and computer networks at the heart of the technology have increasingly converged at a rapid pace^{xv}, and many companies provide unified services, under single ownership, distribution, or management.

Manufacturing is considered a more ‘traditional’ part of the ICT industry, and the complex network of the ICT supply chain involves numerous levels of suppliers comprising tens of thousands of individual companies, beginning at the extraction site for minerals and other raw materials through to sub-assemblies, final assembly, and ending at the point of sale by an original equipment manufacturer (OEM). Up to 80% of global ICT production has been outsourced by brand name companies to contract manufacturers.^{xvi} Five contract manufacturers produce electronics products for all of the major OEM companies, each employing tens of thousands of employees and representing billions of dollars in annual revenues.^{xvii}

3. KEY HUMAN RIGHTS IMPACTS

This section sets out a range of adverse human rights impacts that may result from the activities or relationships of companies in the ICT sector, as identified through multistakeholder interviews and research to date. The term “adverse human rights impact”, in line with the definition used in the UN Guiding Principles, is used to mean an action that removes or reduces the ability of an individual to enjoy his or her human rights. Under the UN Guiding Principles, the responsibility of business enterprises to respect human rights encompasses all internationally recognised human rights – understood, at a minimum, as those expressed in the [International Bill of Human Rights](#) (the Universal Declaration on Human Rights, the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights) and the principles concerning fundamental rights set out in [the International Labour Organization’s Declaration on Fundamental Principles and Rights at Work](#). The commentary to Guiding Principle 12 also makes clear that, depending on circumstances, businesses may need to consider additional international standards, for example, where they may impact upon individuals belonging to groups or populations at heightened risk of vulnerability or marginalisation.

3.1 Impacts on freedom of expression

The right to freedom of expression is often seen as an ‘enabling’ right both in the fulfillment of many other human rights and in exposing human rights violations. The right is not absolute and may therefore legitimately be subject to restrictions to respect the rights or reputations of others, or for the protection of national security, public order (*ordre public*), public health or morals^{xviii}. Impacts on freedom of expression can occur where a disproportionate or unjustified action is taken to restrict free expression. This may occur as a result of the actions listed below.

3.1.1 Blocking, filtering and removing content

To protect other human rights, particularly those of potentially vulnerable groups, states may legitimately impose restrictions on freedom of expression in line with international human rights standards. Child pornography, incitement of racial hatred, and threats of imminent violence are commonly identified as violations prompting the blocking, filtering, and removal of online or other content. However, impacts on free expression occur where such measures are taken in order to prevent legitimate information being publicly displayed, shared, or distributed. Restrictions fall into two categories, those prescribed by law (including via a court order to undertake the restriction or via provisions on intermediary liability), or by companies implementing terms or service as per their own policies.

Governments have increasingly placed “intermediary liability” on companies that provide Internet access, so that in effect they bear responsibility if they host content that the state considers illegal or third parties find offensive. Stakeholders reported that state demands to filter, remove or block content have often been viewed, including by companies, as politically

motivated, lacking adequate notification and justification to users, and requested without due process of law^{xix}. Companies can be faced with fines or the revocation of their legal license to operate in countries where they refuse to comply; or with the prospect of unjustifiably impacting the rights of users who are targeted by the government, leading sometimes to complaints or lawsuits against them.^{xx}

In the absence of global online governance standards, companies have developed their own standards to regulate user behaviour based on their own philosophy or policies, which may or may not be considered consistent with international human rights standards by other stakeholders. Individuals' freedom of expression is typically seen as being unduly restricted for example when content is removed without their knowledge and/or where company decisions to remove content are not justified on the basis of clear policies regulating user behaviour. One assumption behind companies' approaches to these situations appears to be the availability of alternative spaces to which users and content creators can turn. However, in countries where monopolies or oligopolies are in place, cost barriers or lack of alternative service provision can impact on individuals' freedom of expression.

Acting on court orders to enforce copyright laws, copyright owners have managed to block websites in numerous jurisdictions. While protection of intellectual property is a legitimate goal, in several instances such actions have been widely considered a violation of free expression.^{xxi} Copyright laws can pose a challenge from the perspective of freedom of expression if implemented in such a way that such laws increase intermediary liability and make private companies responsible for "policing" content on the Internet, which can lead to abuses in the form of adverse impacts and consequences for freedom of speech. According to stakeholders, this is leading to companies implementing terms of service which go considerably beyond what is legally permissible. Some felt that governments should not abdicate their responsibility, and should not place disproportionate liability provisions on intermediaries which end up creating incentives for such companies to remove content.

3.1.2 Blocking and disconnecting users and access to networks

Governments have demanded blocking access to data or mobile communications in times of civil unrest^{xxii}. Companies that refuse to comply run the risk of losing their legal license to operate, while compliance raises risk of lawsuits from individual users and other challenges. Governments have also given orders to disconnect an entire network (both Internet and telecommunications), such as in Egypt in 2011. According to credible media reports highlighted by stakeholders, such experiments have also been conducted elsewhere, including the deployment of the so-called 'kill switch' to prevent information that the state seeks to control from getting out. Telecommunication industry stakeholders note that this raises a specific business challenge, since some licensing agreements may require compliance with such conditions.

3.2 Impacts on freedom of assembly and association

The denial of freedom of association violates labour rights, which are outlined later in this paper. But the freedoms of assembly and association have important online implications. When governments place restrictions on individuals gathering in public spaces, the Internet can offer a safe alternative space for individuals and groups to assemble and express themselves, including in relation to views that are in opposition to those of the government. By imposing surveillance, intercepting messages, monitoring conversations, and blocking sites online, governments can prevent people from assembling peacefully in a virtual space. When companies provide

governments with the hardware or software to take those actions are often viewed as contributing to these violations (see also section 3.3.3).

3.3 Impacts on the right to privacy

ICT companies often have access to sensitive data about their users' personal information, tastes and habits. Sharing or marketing users' data without consent is frequently reported by stakeholders as an abuse of users' right to privacy, for example in connection with the following activities.

3.3.1 Storing and sharing user data

Data on consumers' behaviour patterns, preferences, billing information and other 'remembered' online information can be improperly used by companies that store the data, whether for commercial purposes or otherwise, and/or illegitimately accessed and misused by the state and other companies. Stakeholders reported cases of companies sharing user data with governments that have ended in the arrest and imprisonment of individual users. Often these users are political or religious dissidents or activists, or media professionals, exercising their right of expression under Article 19 of the International Covenant on Civil and Political Rights.

Further, with consumers and businesses increasingly relying on 'cloud' computing^{xxiii}, huge amounts of data are cheaply stored and accessible anywhere (and not necessarily on specific equipment) for long periods of time. The human rights implications of unjustified government demands to access these data stores may be significant. Stakeholders are also concerned that users who lack sufficient information about the implications of data storage may consent to the storing of their information without being adequately 'informed'.

3.3.2 Preclusion of Anonymity

Requiring users' real names and personal information is often justified on the basis of controlling online actions which may impact on other users. However, anonymity is also seen by many stakeholders as an online mechanism that protects them from abuses. The use of individuals' personal information to target their activities or associations for illegitimate purposes (see below) or without due process of law can impact their right to privacy.

3.3.3 Enabling surveillance

International human rights law recognises that states may have legitimate reasons to place certain individuals or groups under surveillance following due process of law, for example when their actions are suspected to be criminal. However, where this is not the case, this impacts not only individuals' right to privacy but also freedom of expression. Companies are required to cooperate with competent legal authorities regarding lawful interception. But stakeholders report that some governments have abused the mechanism. For example, governments have inappropriately required access to user data or specific use of surveillance software to target political or human rights activists, and purchased products, or demanded companies tailor products, or technology to enable surveillance, Internet traffic monitoring, and communications intercepts which may violate international human rights standards. If individuals are unaware of the surveillance, during or after the surveillance has ended, they may face prosecution for exercising their right to free expression; if they do suspect surveillance they may censor themselves, affecting their right to free expression, as well as free association with other people on the Internet. Companies are often viewed as contributing to these violations where they provide governments with the hardware or software to carry out the surveillance.

3.4 Impacts on Labour Rights

Civil society stakeholders stressed that these impacts can occur as a result of company activities throughout the value chain but can be particularly acute in the ICT supply chain. Stakeholders observed that workers throughout the sector's supply chain often face involuntary overtime, working excessive numbers of days in a row or for prolonged periods in one day without adequate time to rest. Frequent cases have been documented of work regimes and workplace rules requiring employees to spend excessive time in one position or completing repetitive tasks, leading to adverse health impacts. Disciplinary measures adopted to ensure compliance with these rules are in some instances considered inhumane treatment. Exposure to toxic chemicals and hazardous materials is reported by some stakeholders as a continuing danger in factory production environments as well as in recycling operations.^{xxiv}

3.4.1 Impacts arising from the growth in agency labour

Agency, contract, or 'outsourced' employment, typically recruited, supplied and employed by a private sector employment agency, constitute a significant proportion of the global ICT manufacturing workforce and is reportedly on the rise. Some stakeholders noted that the 'triangular' nature of the relationship between a company, agency and worker may leave workers outside the scope of protection of local labour laws due to lack of clarity over which organisation is the legal employer. Young women and migrant workers who are especially vulnerable to adverse human rights impacts are prominent in this workforce. Where migrants have been recruited or employed by agencies or hired directly by companies, they may be particularly vulnerable to adverse human rights impacts, including on their freedom of movement (where agencies sometimes retain identity documents or make illegal deductions to wages or illegally impose fees associated with securing their employment). In the worst cases, this might include forms of bonded or even forced labour. Migrant workers can also find it particularly difficult to access effective remedies through the domestic legal system.

3.4.2 Impacts on freedom of association

Stakeholders reflected that trade unions were not much in evidence within the ICT manufacturing sector, call centres and shops. Lack of such representation may lead to a circumvention of workers' ability to lodge grievances and seek redress for adverse impacts. Some stakeholders noted that where there is insecurity of tenure for the agency worker and/or frequent changes in worksite, risks to the rights to freedom of association and collective bargaining may be heightened. Civil society stakeholders noted that there may also be impacts on the ability of user enterprise employees to organise. Industry stakeholders emphasised that there should be no assumption that it is more difficult for agency workers to exercise these rights.

3.5 Other impacts in the value chain – from sourcing and disposal

3.5.1 "Conflict minerals"

Physical attacks and sexual violence committed against civilians by armed militias, forced and child labour, and health impacts resulting from environmental degradation are some of the widely recognised adverse human rights impacts associated with the extraction, trade, and transport of certain minerals, particularly from conflict zones, that are used in the production of most ICT products. Industry stakeholders stressed that sourcing conflict minerals is a challenging issue across a wide range of sectors, not just ICT.

3.5.2 Impacts related to e-waste

Developing countries receive the bulk of the 'e-waste' associated with ICT products that have been discarded by users, and often lack sufficient capacity and infrastructure to ensure the safe disposal or recycling of hazardous material^{xxv}. Workers and scavengers (often children) of the sites and residents of local communities can face severe risk of illness and, frequently, of health impacts resulting from environmental contamination due to the often inadequate methods used to break down and separate the waste and exposure to heavy metals and possible carcinogens.

4. CONTEXTUAL FACTORS

Stakeholders emphasised that the activities of companies must be understood within the wider contexts in which they operate, and which may increase the risk of some of the above human rights impacts occurring. The following contextual factors were highlighted by different stakeholders:

4.1 Global reach without global regulation

Among industrial sectors, the ICT sector has certain unique characteristics of technical complexity and speed of development, which adds to the challenge of identifying and assigning responsibility for specific actions. There are several specialised agencies or organisations to help navigate the issue. For example, a non-governmental organisation called the International Corporation for Assigned Names and Numbers (ICANN)^{xxvi} coordinates the Internet domain name system's architecture and structure. The International Telecommunications Union (ITU) sets standards for telecommunication industry, and the Internet Governance Forum provides space for multistakeholder policy dialogue.

While the sector includes and relies upon communication services that have typically been seen as a public good, the leading global actors are from the private sector and much of the infrastructure is private, yet almost all governments regulate the ICT sector through national laws and in many countries, the government itself, or state-owned enterprises, exclusively or competitively manufacture equipment or offer services. The many parts of the ICT industry that transcend borders, including the Internet and social media platforms, may be subject to overlapping and conflicting regulation – or none at all. Compounding this unique governance environment is the fact that new technologies, products, services and business models within the sector often develop much faster than regulators can react to them.

4.2 Government violations

Some companies in the ICT sector have to manage a close and active relationship with governments and law enforcement agencies. As noted above, under specific circumstances, such as imminent threat of violence, states have an obligation to prevent such violence and can impose restrictions on individuals' freedom of expression and right to privacy for this purpose. Restrictions can take the form of targeted surveillance, using court-ordered judicial intercept mechanisms, seeking information about individuals or groups operating in anonymity and prosecuting them if their conduct harms the human rights of others. However, private companies are increasingly faced with difficult choices in responding to such government requests, where imposing surveillance is not in line with international standards and these appear intended for purposes with adverse consequences for human rights, such as those described in section 3.1 above. The challenge may be particularly acute where the request is accompanied by the intimidation of local company employees. Yet companies have been widely criticised by stakeholders for acceding to such requests without much resistance, or continuing to sell such surveillance technology to governments with a record of utilising it to violate human

rights. While some governments are actively adapting technology to make use of new means of surveillance, some companies are marketing and selling surveillance technologies that are not compatible with international human rights standards.

4.3 Bribery and corruption

Considering the close relationship companies in the ICT sector are required to have with governments and law enforcement agencies, and given that the sector often requires government licenses and contracts to operate, there is a high risk of bribery and corruption in countries with weak governance. Stakeholders mentioned there were strong frameworks in place to address these issues, such as the US's Foreign Corrupt Practices Act, the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions and the UN Convention Against Corruption. Some stakeholders noted that in many countries corruption interferes with labour rights, especially freedom of association.

4.4 Regulatory approaches to conflict minerals

Recent regulatory initiatives have sought to require companies to have greater insight into minerals sourcing from conflict zones associated with gross human rights abuses. §1502 of the U.S. Wall Street Reform and Consumer Protection Act (popularly known as the Dodd-Frank Act) requires companies purchasing certain minerals from the Democratic Republic of Congo (DRC) to disclose measures taken to exercise due diligence on the source and supply chains of specific resources associated with conflict in the region. Stakeholders report conflicting views as to whether the appropriate way forward lies in further binding legislation or through voluntary but targeted industry coordination.

5. KEY PROCESS CHALLENGES

The UN Guiding Principles set out a number of process steps companies are expected to take as part of their responsibility to respect human rights. Stakeholders were asked to identify challenges, barriers and opportunities in relation to each of these steps, taking account of adverse human rights impacts that may arise through companies' own activities or through their business relationships. A range of issues were identified in stakeholder interviews, which are summarised below.

5.1 Embedding respect for human rights in a company

The UN Guiding Principles observe that a business's policy commitment to respect human rights should be embedded from the top of the enterprise through all its functions, which otherwise may act without regard for human rights. This requires coherence between the human rights policy and other policies and procedures that govern its wider business activities and relationships.

Issues identified by different stakeholders included the following:

- Allegations that companies in the sector have been involved in acts that suppress human rights, particularly by governments, have challenged assumptions that the sector has a purely positive impact on human rights by enabling people to connect, express themselves and promote democracy. This has led many to see a need for companies to have better human rights policies to guide their staff in dealing with these challenges.
- There is a perceived need for clarification about key human rights such as freedom of expression and association and privacy given their complexity and the well-developed jurisprudence in many jurisdictions. This may help companies navigate their way through government requests. Moreover, differences between jurisdictional requirements may lead

companies to behave differently in their home and host states.

- Embedding human rights considerations and thinking about human rights implications from the beginning of a start-up company's operations was seen as invaluable by stakeholders, with human rights becoming an integral part of how companies will operate in the future.

5.2 Assessing risks to human rights

The UN Guiding Principles state that businesses should identify and assess any actual or potential adverse human rights impacts with which they may be involved either through their own activities or as a result of their business relationships. This includes assessing the human rights context prior to a proposed business activity, where possible; identifying who may be affected; cataloguing the relevant human rights standards and issues; and projecting how the proposed activity and associated business relationships could have adverse human rights impacts on those identified. Importantly, human rights risks to people impacted as a result of the business's activities or its relationships should be considered separately from any risks to the business that may flow from its involvement with human rights impacts. However, the two are increasingly related.

Issues identified by different stakeholders included the following:

- Using new and evolving technologies for purposes other than those originally intended, and which may harm human rights, is seen to be a particular risk for the ICT sector. It is not always easy for companies to anticipate what these uses may be. This is a concern also for intermediary suppliers when customers reengineer products to abuse human rights.
- The depth and scope of risk assessment required is a key concern for industry stakeholders, especially in government relationships in countries lacking strong rule of law. The rapid changes in technology may require companies to re-assess how frequently they should be reviewing their impacts as well as their guidelines and other systems for managing them.
- Companies are under increasing pressure from other stakeholders to be more transparent about the processes by which they assess human rights risk and report to the public, or at least key stakeholders.
- Existing supplier auditing programs are perceived by some as inadequate in assessing and addressing human rights impacts on agency workers in particular. Some stakeholders viewed the Electronic Industry Citizenship Coalition (EICC) Code of Conduct regarding forced or bonded labour and related practices^{xxvii} as good practice. Others noted that OEM auditing programs typically fail to include the recruitment and employment standards used by agencies that supply them with workers^{xxviii} and fail to identify violations of the right to freedom of association.

5.3 Integrated, cross-functional decision-making to address human rights impacts

The UN Guiding Principles state that in order to prevent and mitigate adverse human rights impacts, businesses should integrate the findings from their impact assessments across relevant internal functions and processes, and take appropriate action in order to prevent and mitigate the impacts identified. Integration requires internal decision-making, budget allocations and oversight processes that enable effective responses to such impacts.

Issues identified by different stakeholders included the following:

- Many stakeholders see a need for companies to develop and follow certain set procedures when faced with human rights challenges, including whether and when companies can or should refuse to comply with government requests or judicial orders. Stakeholders identified the need to invest in staff who have the necessary skills, including a firm understanding of

the human rights implications and law around take-down procedures and data privacy, and the need for staff to be supervised by senior level management with clear lines of responsibility. Other key actors identified as necessary to decision-making on human rights issues were lawyers, technological experts, as well as external stakeholders. Support for local management on the ground was also stressed.

- Some stakeholders noted the importance of carrying out due diligence going into new investments or situations so that companies will be better able to appropriately respond if or when government requests come in.
- Industry stakeholders noted that decisions often have to be made very quickly in response to government requests for blocking and disconnecting websites. The time limit governments set for a range of requests of this kind was reported to vary between 20 minutes and five hours. Within this timeframe companies must assess the legality of the request under international and domestic standards, which requires a well-coordinated response. One stakeholder noted that interception requests were a daily occurrence in some countries where a legal framework for lawful interception is absent.
- Stakeholders highlighted inconsistencies in policies and practices across company departments, in particular between company procurement practices and human rights objectives. This was seen as related to the auditing challenge identified above.

5.4 Human rights impacts of business relationships in the sector

The responsibility to respect human rights under the UN Guiding Principles encompasses adverse human rights impacts that may occur as a result of a company's business relationships with third parties. This includes adverse impacts that are directly linked to its operations, products or services by a business relationship, even where it has neither caused nor contributed to the impact itself. When identifying how best to address impacts that result from its business relationships, the company's leverage will be a significant factor. Leverage refers to the ability of the company to effect change in the wrongful practices of another party that is causing or contributing to an adverse human rights impact. Using leverage may involve working with the entity most directly responsible for the impact and/or with others who can help.

Issues identified by different stakeholders included the following:

- Stakeholders noted that due to the fast paced nature of technology, leverage in the ICT sector changes significantly, rapidly and unpredictably. At the same time, many countries have newly installed or updated communications networks and are seen as failing fully to realise the extent of the powers they control. Some stakeholders recommended lobbying such governments on the benefits of human rights protection, although this raises its own challenges.
- Many stakeholders also noted that the ICT sector exists as an 'ecosystem' in which multiple companies rely on each other to bring a product or service to market. This may create barriers or opportunities for leverage in support of human rights. Other stakeholders conversely identified this as an opportunity for cooperation to address 'larger' human rights impacts.
- Telecommunications industry stakeholders are bound by license agreements with governments to operate in a territory and as such feel they have very little power to do other than abide by the legal and regulatory framework as it is.
- Stakeholders report that, outside of certain industry association-led efforts, OEMs' anti-trust concerns often prevent them from collaborating with other OEMs to jointly approach suppliers who have adversely impacted human rights or have failed to take remedial action. Others noted that companies in other industries, such as apparel, and even initiatives

within the sector, do not seem to face the same constraints.

- Stakeholders noted that the (real or perceived) limited visibility within OEMs' supply chains – largely to Tier 1 suppliers alone – further limits the potential for effective leverage through collective action.^{xxix} Some observed that the recent US Dodd-Frank Act and its due diligence requirements have begun to provoke new thinking, forging closer working relationships within the supply chain.

5.5 Measuring effectiveness of company responses to human rights impacts

The UN Guiding Principles underline the need for companies to track the effectiveness of their responses to adverse human rights impacts (whether actual or potential impacts) in order to verify whether the impacts are being addressed effectively. Tracking should be based on appropriate qualitative and quantitative indicators and draw on feedback from both internal and external sources, including affected stakeholders.

Issues identified by different stakeholders included the following:

- Stakeholders described methods for measuring the human rights compatibility of content 'takedown' policies whereby samples of removed content are reviewed monthly and analysed to see whether the original removal decisions were in line with legal obligations and relevant company guidelines. The tracking of 'reversal rates' (whereby online content has been removed and later reinstated) was also seen as an important tool to measure effectiveness of company policy and practice with regard to the removal of content.
- One stakeholder said companies should maintain records in relation to content taken down where criminal allegations are involved, especially if there were subsequent prosecutions and if law enforcement authorities requested access to log files associated with the alleged criminal activity.
- Various stakeholders report that in order to avoid overly censoring content, takedown must be on a case-by-case basis and must be carried out by people, i.e. not automated, in order to appreciate the context in which some footage is uploaded. Many stakeholders take the view that using an algorithm cannot substitute for context, and keyword filtering can be overly broad.
- Limitations noted above (see section 5.2) with regard to supply chain auditing, including and particularly in relation to agency workers, are also seen as limitations on the ability to measure the effectiveness of efforts to support respect for labour rights in ICT supply chains.

5.6 Stakeholder engagement in addressing human rights impacts

Stakeholder engagement is a cross-cutting theme within the UN Guiding Principles, particularly in the context of assessing impacts, tracking responses, providing for adequate communication about how impacts are addressed, as well as in the remediation of impacts. The UN Guiding Principles recognise that not all companies will be able to consult directly with those groups who may be impacted (for instance due to legitimate resource limitations), but that where this is not possible, other avenues should be sought to understand their likely perspectives and human rights concerns.

Issues identified by different stakeholders included the following:

- Many stakeholders consider that companies in the ICT sector should engage more directly with civil society in social partnerships and dialogue and build 'trust relationships' with grassroots organisations, though some were unsure how to open channels of communication to start relationships.
- Some companies operate their own pool of 'trusted advisers' made up of user groups and

NGOs who they remain in contact with and rely on to flag up problems with content arbitrarily being taken down or confirming the legitimacy of an activist or other civil society group.

- Some civil society stakeholders highlighted the need for companies to engage in more meaningful disclosure to customers, providing clearer terms and conditions and an enhanced level of dialogue with users over reasons why online content has been removed.
- Some stakeholders stressed the need to educate users in how their online actions can impact human rights.

5.7 Complaints handling / grievance mechanisms (by a company)

The UN Guiding Principles state that where businesses identify that they have caused or contributed to adverse human rights impacts, they should provide for or cooperate in their remediation through legitimate processes. They also provide that business enterprises should establish or participate in effective operational-level grievance mechanisms for individuals and communities who may be adversely impacted, in order that grievances may be addressed early and remediated directly.

Issues identified by different stakeholders included the following:

- The need to address grievances before they escalate through effective redress mechanisms.
- In relation to labour disputes, it was observed that some companies are reluctant to open a dialogue with bodies that may be well-placed to assist in the negotiation and resolution of grievances. The use of Ombudsman offices to settle internal employee disputes was suggested as a form of best practice to apply across the sector. Stakeholders stressed that company grievance mechanisms should not be used to undermine the role of legitimate trade unions in addressing labour-related disputes.
- Transparency was identified as a critical factor in addressing grievances. It was suggested by some stakeholders that companies should account to users on at least an annual basis on grievance-handling processes. Others identified a tension between civil society's need for transparency and the company's need to keep some details of activities confidential, particularly to protect local employees.
- Some stakeholders suggested that companies should educate users on the potential human rights impacts of using their services, such as notifying users that they may be legally monitored according to the laws of the governing state.

6. NATURE OF THE GUIDANCE

Initial research and interviews with stakeholders have identified the following views on the potential focus and form for the forthcoming guidance. At this early stage there is no consensus about the exact content or form that the guidance should take.

Stakeholders identified a number of areas where they would like to see clarification on sectoral issues, including:

- the human rights standards that apply, clearly setting out the issues and what steps can be taken to mitigate risks;
- whether specific criteria should be applied to human rights risk assessments;
- how a company should “balance” freedom of expression with other rights, as well as how to “balance” human rights with requirements imposed by law enforcement agencies;
- how companies across the sector can find consistent ways to address censorship;
- what an appropriate standard of privacy looks like to assist the sector in moving away from opt-out provisions;

- the appropriate level of transparency needed around terms of service;
- how companies can address human rights in the long term and engage with civil society more directly.

With regard to the supply chain, some stakeholders suggested that the guide should:

- provide practical, concrete steps that demonstrate how due diligence ought to be performed, and how companies can mitigate any adverse human rights impacts that might result from their business operations or those of their suppliers;
- be viewed by companies as having been ‘co-developed’ by them, with suppliers clearly understanding that it takes into account their voice as a stakeholder in the process;
- clarify why and how human rights due diligence is directly applicable to contract manufacturers and other suppliers in the OEM supply chain, as opposed to current perceptions that due diligence and the responsibility to respect human rights are a priority of OEMs alone.

Stakeholders also suggested variously that the guide should:

- Identify sectoral areas that have clear guidelines and areas where further work is needed;
- Tackle the emerging issues and challenging areas that have not significantly been addressed (for example, the debate over equipment being used for blocking/filtering and surveillance, either intentionally or because of the ‘dual use’ nature of the technology, and the implications for the corporate responsibility to respect);
- Encourage company sharing of best practice;
- Encourage statements, initiatives and commitments from the EU, UN and other regional and international organisations in support of human rights within the sector, which could reinforce companies’ responses when faced with the risk of involvement with human rights violations.

Stakeholders drew attention to the following existing initiatives in particular:

- Electronic Industry Citizenship Coalition (EICC)^{xxx}
- The Global e-Sustainability Initiative (GeSI)^{xxxi}
- The Global Network Initiative (GNI)^{xxxii}
- The Industry Dialogue^{xxxiii}

ANNEX A

Project Background

In October 2011, the [European Commission](#) adopted a new [Communication on Corporate Social Responsibility](#) that defined corporate social responsibility as “the responsibility of enterprises for their impacts on society”. As one of the priority actions in the business and human rights field, the European Commission committed to developing guides for three industry sectors on the corporate responsibility to respect human rights under the [UN Guiding Principles on Business and Human Rights](#). After a brief public consultation requesting input on the sector selection according to a set of [publicly available and objective criteria](#), the Commission selected the Employment & Recruitment Agencies, Information & Communication Technology, and Oil & Gas sectors as the focus of the guides.

While the guides will take particular account of the situation and experiences of EU business, they aim to be as globally relevant as possible in order to contribute to a harmonised approach to the implementation of the Guiding Principles. The development of the guides will mirror, on a smaller scale, the approach taken in developing the Guiding Principles: being global in approach and informed by relevant evidence and the views of a wide range of stakeholders, including representatives from business, civil society, trade unions, government, and other experts. The guides will be based on research, extensive interviews with diverse stakeholders (75+ per sector), and inputs from two multistakeholder roundtables per sector. The European Commission's [Expert Advisory Committee](#) and three multistakeholder [Sector Advisory Groups](#), convened specifically for the project, are providing strategic advice and feedback.

Project Timeframe

- January – March 2012: Consultation on and finalisation of sector selection, formalisation of EC Expert Advisory Committee and Sector Advisory Groups; appointment of sector-specific researchers.
- April – August 2012: Ongoing consultation with broad range of stakeholders through in-depth confidential interviews (including select country visits) and first set of multistakeholder sector Roundtables hosted by the EC, as well as additional desk-based research.
- September – November 2012: Guide drafting phase, further specific research as needed, and second set of multistakeholder sector Roundtables hosted by the EC to discuss the draft guides.
- December 2012: Submission of the three guides to the EC and finalisation for publication.

The UN Protect, Respect, Remedy Framework and the UN Guiding Principles on Business and Human Rights

In June 2011 the UN Human Rights Council unanimously endorsed the UN Guiding Principles, establishing the first authoritative global standard on the respective roles of business and governments in helping ensure that companies respect human rights in their own operations and through their business relationships. They spell out the implications of the three pillars of the [UN 'Protect, Respect, Remedy Framework'](#) on business and human rights. The UN Guiding Principles were developed by the Special Representative to the UN Secretary-General for Business and Human Rights, Professor John Ruggie, over the six years of his mandate. Based on extensive research and consultations with representatives from government, business, civil society, trade unions and legal and academic experts across all continents, the UN Framework and UN Guiding Principles gained broad acceptance and support. The responsibility of business enterprises to respect human rights encompasses all internationally recognised human rights – understood, at a minimum, as those expressed in the [International Bill of Human Rights](#) and the principles concerning fundamental rights set out in the [International Labour Organization’s Declaration on Fundamental Principles and Rights at Work](#).

END NOTES

ⁱ See: <http://www.ihrb.org/project/eu-sector-guidance/index.html>

ⁱⁱ See for example the OECD's definition of the ICT sector:

<http://www.oecd.org/dataoecd/34/37/2771153.pdf>

ⁱⁱⁱ These devices can create, receive, compute, and communicate, such as Apple's iPhone, Samsung's Galaxy, etc.

^{iv} Such as desktop computers, laptop computers, tablets and netbooks such as by Dell, Apple, Hewlett Packard, Toshiba, Lenovo, Acer, etc.

^v Such as those made by engineering companies like Siemens or telecom equipment manufacturing companies like Ericsson.

^{vi} Comprising a vast, competitive sector comprising many small manufacturers who supply larger customers, but also large-scale manufacturers, such as WorldCom (which merged with MCI, and is now part of the Verizon group).

^{vii} Which stores and passes along the data on the right path at high-speed through complex network systems and switching equipment, such as Cisco.

^{viii} Including telephone companies (Such as AT&T, BT, or Deutsche Telekom, as well as mobile providers such as Vodafone, Orange, T-Mobile, among many others), cable TV operators (such as Sky in the UK), and other Internet Service Providers (ISPs) (such as BlueWin in Switzerland, the former NTL). Many ISP companies having integrated functions to provide internet, cable TV and telephony however, making such clear distinctions within the sector almost redundant.

^{ix} Popularly known as 'clouds', provided on both individual and commercial bases, such as iCloud from Apple or DropBox for personal users, and integrated solutions for corporations from companies like SAP and Amazon.

^x Such as blogging enablers, like Blogger, Blogspot, Tumblr.

^{xi} Such as social networking sites, like Facebook, Twitter, Google+.

^{xii} Such as Google's Chrome, Microsoft's Internet Explorer, Mozilla's Firefox.

^{xiii} Such as Google, Yahoo!, Bing (a product of Microsoft), and the former AltaVista.

^{xiv} Such as Microsoft or Apple's Mac-based systems.

^{xv} One popular aphorism in the sector is the Moore's Law, which says that the number of transistors that can be placed in an integrated circuit doubles every two years. It has become the metaphor for rapid changes, even planned obsolescence, in which manufacturers introduce new products at regular intervals with sufficient new features to make earlier versions less attractive to consumers. Software development is similarly rapid.

^{xvi} See Schipper, Irene, and Esther De Haan. *CSR Issues in the ICT Hardware Manufacturing Sector*. Rep. SOMO, 2005 at <http://somo.nl/>

^{xvii} Foxconn for example, the world's largest CM, employs more than 126,000 employees and reported 2011 revenues of approximately \$5.7 billion USD.

^{xviii} Article 19 of the International Covenant on Civil and Political Rights (ICCPR) states:

1. Everyone shall have the right to hold opinions without interference.

2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

(a) For respect of the rights or reputations of others;

(b) For the protection of national security or of public order (ordre public), or of public health or morals.

^{xix} According to Google, of the 355 take-down notices the Indian Government sent Google in a six-month period in 2011, some 258 dealt with controversial, but legal content which was political in nature (including satire) and the company refused to comply with all the requests. See: <http://www.google.com/transparencyreport/>.

^{xx} Realising that companies cannot monitor every file that users upload, most governments allow companies a "safe harbour" provision, reducing their liability in good faith situations where they persist in

hosting content that the state or legal authority has required be taken down due to public interest or security.

^{xxi} For example, when artists, musicians, writers, or cartoonists have used copyrighted material and manipulated it to create a new distinct work of art.

^{xxii} For example: During the Egyptian Revolution in 2011, the Egyptian Government asked companies providing Internet access and cellular telephony to suspend services, citing its emergency powers. All companies complied. After the riots in England last summer, the British Government sought – and then decided against seeking – access to data from hand-held communication devices, such as smartphones. In Karachi, Pakistan, cellphone usage has often been barred for long periods, and in the Indian-held Kashmir, the government has imposed controls on mobile communication technology, ostensibly to curb terrorism or crime.

^{xxiii} The storage of password protected data on dedicated servers in multiple geographic locations.

^{xxiv} For example, the Fair Labour Associations' recent inspection report concerning conditions at several factories in China, identifying worker concerns about metallic dust and the potential for explosions as a significant concern.

^{xxv} It was reported that upwards of 50 million metric tons of discarded ICT products known as 'e-waste' is generated each year, mostly by countries in Europe and the United States, sent to amass in dumping grounds in Nigeria, China, Ghana, and India.

^{xxvi} ICANN is empowered with the task of coordinating the Internet's system of unique identifiers so that it operates in a stable and secure manner. It is a nonprofit organization headquartered in the United States.

^{xxvii} This states that: "Forced, bonded (including debt bondage) or indentured labor, involuntary prison labor, slavery or trafficking of persons shall not to be used. This includes transporting, harboring, recruiting, transferring or receiving vulnerable persons by means of threat, force, coercion, abduction or fraud for the purpose of exploitation. All work must be voluntary and workers shall be free to leave work at any time or terminate their employment. Workers must not be required to surrender any government-issued identification, passports, or work permits as a condition of employment. Excessive fees are unacceptable and all fees charged to workers must be disclosed."

^{xxviii} Except, see Apple's 2009 Supplier Responsibility Progress Report:

http://images.apple.com/supplierresponsibility/pdf/Apple_SR_2009_Progress_Report.pdf

^{xxix} The issue of supplier visibility stems, in part, from a historic tendency on the part of sector to treat as confidential all information about suppliers. Of the major brands, only HP and Apple have released a list of key suppliers. And in both cases the information is limited to the name of the supplier. No information, for example, is provided as to the location of specific factories where OEM products are manufactured.

^{xxx} The EICC is a coalition of the world's leading electronics companies working together to improve efficiency and social, ethical, and environmental responsibility in the global supply chain. The EICC code of conduct can be accessed here: http://www.eicc.info/eicc_code.shtml

^{xxxi} GeSI is a collaboration of company members and associate members dedicated to ICT sustainability through innovation. GESI initiatives can be accessed here: www.gesi.org

^{xxxii} The GNI is a multistakeholder initiative established to advance freedom of expression and privacy in the ICT sector. The GNI Principles, Implementation Guidelines and Governance, Accountability and Learning Framework can be accessed here: <http://globalnetworkinitiative.org/>

^{xxxiii} The Industry Dialogue is a collaboration between twelve telecommunications companies established to address human rights impacts and share best practice.