Keynote speech by John Morrison  
Deutsche Telekom Sustainable Procurement Dialogue Day  
Bonn, 26th March 2014  

Business and Ethics in Globalized Value Chains –  
To what extent is ethical responsibility enforceable and manageable?

I would like to thank Deutsche Telekom for inviting The Institute for Human Rights and Business to make this keynote speech at the Sustainable Procurement Dialogue Day. In the next minutes I would like to reflect with all of you on five key questions:  
- Why are human rights necessary for the social sustainability of any business?  
- What trends will the ICT sector need to address in this area in the time ahead?  
- How should any ICT business be thinking about human rights issues?  
- What are some of the good practices emerging?  
- And, where will we be in five years time?

1: Why are human rights a central part of social sustainability for any business?

The relationship between telecommunications companies and the enjoyment of human rights has been overwhelmingly positive over the past twenty years. Digital communications have become a valuable tool in fostering greater realization of many human rights. For example, people in rural Africa are better able to conduct economic transactions; farmers can more easily find the price of their crops; in India, people use mobile technology to undertake vigorous political discussions; in many other countries activists are increasingly able to bypass censors to have conversations that were otherwise impossible; and as we saw in Egypt and elsewhere in North Africa three years ago, peaceful demonstrators are able to mobilise against authoritarian governments.

The developments in Information and Communication Technologies, or ICTs, over the past few decades have led to fundamental changes in the way we work, socialise, learn and do business. ICTs are deeply integrated in almost every part of our daily lives. Investment and innovation has made this possible and contributed to
the enjoyment of rights such as freedom of expression, the right to participate in political processes, as well as rights to information, education and healthcare. There is little doubt that, driven mainly by the private sector, the development of digital communications and the Internet has had a largely beneficial effect both in economic and social terms.

But new challenges have emerged. We’ve all seen how information technology can be used by some governments against the very people whose rights they are meant to protect, and who the technology is intended to benefit, and the complex supply chain can be fraught with risk often unseen by the company. For example, the same technology that can track down survivors of an earthquake based on the telephone signals they emit can also be used by a government to track down political dissidents at a peaceful protest.

In order to tackle these challenges, business needs a common set of benchmarks to understand its risks, impacts and opportunities across international markets and along its whole value chain.

During the past fifteen years, consensus began to emerge on how the broad international human rights framework should relate to the business sector. We saw this through the evolution from the broad principles of the UN Global Compact to the more precise due diligence framework found in the UN Guiding Principles on Business and Human Rights endorsed unanimously by the UN in 2011. The Guiding Principles are now also incorporated into the OECD Guidelines for Multinational Enterprises, the European Union CSR Communication, the ISO 26,000 social responsibility standard and increasingly within the Global Reporting Initiative.

Efforts to translate the Guiding Principles into ICT sector operations are now underway. This can be seen through the development in 2012 of the European Commission ICT Sector Guide on Implementing the Guiding Principles on Business and Human Rights, in which Deutsche Telekom took an active role, and in IHRB’s own Digital Dangers project, which identifies risks to human rights in the online world posed through the interplay between business and government, and sometimes other non-state actors.

Also important, there are a number of multi-stakeholder and industry led initiatives that aim to help business along this path, including the Global E-Sustainability Initiative of which Deutsche Telekom is a key member, as well the Global Network Initiative and the Industry Human Rights Dialogue of Telco companies.
2: What trends in the ICT sector will need to be addressed?

We have learned an obvious truth from the interplay between technology and society – that technology is often values-neutral. It can have huge benefits, but also pose significant risks. If we are to apply the precautionary principle in the context of the ICT sector, it is apparent that we have to ensure that the harm technology might cause to human rights should be mitigated, and where necessary, eliminated, so that the positive impacts can be reinforced. Taking that as a basic principle, it means, for example, that supply chains in the manufacturing sector should be free of forced labour, and the extraction of minerals that go into making the components of equipment necessary for the technology to function effectively, must be free of abuse. The recent proposed EU regulation for conflict minerals takes the process forward from the Dodd Frank Act in the United States, which requires companies that use specific minerals to assure stakeholders that the minerals were acquired without fueling conflict. We expect more commodities to face such scrutiny in the future. Such responses to commodity supply chains will have to become more systematic.

While it is true that there is an audit fatigue among companies, the overarching goal – of keeping the supply chain free of conflict is so important, that it cannot be ignored. In his letter to EU President Jose Manuel Barroso, the Chair of IHRB – Professor John Ruggie (author of the UN Guiding Principles) stated: “There is no doubt that reporting – not least for companies many tiers removed from the abusive practices – needs to be targeted, manageable and proportionate. (But) a move to make reporting entirely optional risks leaving the most responsible companies exposed while those least attentive to their human rights responsibilities continue their current practices undeterred. It is surely through requiring the same reporting standards across companies that the Commission can help drive improvements where they are most needed and advance corporate respect for human rights in practice.”

Workers’ rights are also a critical issue that will continue to require greater attention from all actors. While the ICT sector has not seen a disaster of the magnitude of Rana Plaza in Bangladesh, where a building collapsed nearly a year ago, killing close to 1,200 workers, many of them women, we are all familiar with incidents in other places such as China, in factories that supply hi-tech equipment to major brands around the world, where the working conditions were so onerous that they drove some workers to take their lives.

As the ICT sector’s supply chains reach the far corners of the world, it will raise a unique challenge: of applying international standards in settings where all rights are
 Companies will have to deal with suppliers who may be required by law to discriminate against workers of a different faith, ethnicity, national origin, language, or sexual orientation. Companies that are, and aspire to be international leaders, will be expected to live by the highest standards, and push for change.

The ICT sector’s biggest challenges over the coming years will be beyond the supply chain. Companies face key operational dilemmas in many parts of the world, most recently regarding issues such as surveillance, privacy and the possible knock on effects for data storage and transfer. In June 2013, former US defense contractor Edward Snowden leaked documents to several newspapers concerning mass collection and sharing of phone and internet data by the National Security Agency in the US and General Communications Headquarters (GCHW) in the UK. As we all know, these revelations have become the focus of the human rights and business debate in the ICT sector over the past year, besides dominating the broader security and strategic agenda. The importance of “metadata”, and allegations that private companies colluded with state secret services and supplied this data, has put the ICT sector under unprecedented scrutiny. It is also noteworthy that the United States has announced plans to begin to transition its control over the international infrastructure for assigning domain names on the Internet, leading to a possibly more democratic form of Internet governance.

Technology companies based in the US find that their business model has been weakened due to the potential loss of trust in their services. They have begun to distance themselves from programmes like Prism and are strengthening their own data encryption. Elsewhere, companies are positioning themselves as defenders of privacy rights and responding to fears from consumers about using US based services and storing data on US servers, particularly if the US government can get access to that data. Deutsche Telekom, we note, was quick to develop the ‘Email Made In Germany’ service, which offers encryption and storage of data on local servers. But in turn such diffusion of services on the Internet poses its own challenges, including possible balkanisation of the Internet.

The fallout from the Snowden revelations has made consumers worldwide think more carefully about how they use ICT products and services, and has made many governments worldwide ask how they can further control these products and services. Business can often be stuck in the middle – seeking to abide by the law while responding to consumer pressure for enhanced protection against overreaching surveillance in the name of national security. Greater access to the latest communications technologies is good for the human rights activist, the journalist, the social development practitioner; but we must acknowledge it can also help the potential extremist, the terrorist, and the one who wishes to violate others’
rights. Technology that intrudes is values-neutral; technology that offers privacy is also values-neutral. How can we develop tools and techniques that protect those who fight for human rights protection, but make it easier for those whose job it is to protect human rights, to do so?

3: What questions should any business ask itself?

Some of the key questions any business must ask of itself in line with UN, OECD and other corporate responsibility standards are:

- How much knowledge of potentially negative human rights impacts linked to the company’s operations is it necessary for that company to acquire?
- How should the company act on this knowledge?
- How transparent should it be about the knowledge it acquires about these issues?
- How can it ensure there are adequate remedies when there are protection gaps?

To respond effectively, companies will need to know where the greatest risks are and what negative impacts might result in human rights terms.

First, it means companies should make prevention their priority. They must ensure they do no harm. To do so, they need to assess the risks and impacts associated with their technology, practices, and conduct. A company alone may not be able to obtain everything it needs in this area. But it is critical that they make every effort to do so and then to be open with all stakeholders about their conclusions, in order to build a philosophy of transparency, accountability and continuous improvement. There will inevitably be areas where companies will have to be less than transparent – for reasons of commercial confidentiality and security. They will therefore need expert advice so that they arrive at principled, pragmatic decisions.

Second, the issue of remedies. What role does a company have in providing adequate remedies when individuals or groups have been harmed? Should the company play an overtly protective role, or should it help create collective remedies and let an independent authority arbitrate? How does the company function in a state that does not have independent authorities or legal systems that ensure access to effective state based judicial or non-judicial remedies for human rights harms?
4: What good practices are emerging?

Supply Chains

The good news is that good corporate practices are emerging in the area of supply chain management. The bad news is that the practices are not known, and are often cloaked under proprietal confidentiality. What we do know is the following:

- There are now systemic industry-wide approaches to common challenges;
- Common reporting standards are starting to emerge, but there is need for greater alignment;
- There are emerging regulatory requirements, which make it important for the ICT sector to take these concerns seriously.

Operations

The human rights challenges for the ICT sector may seem unmanageable, in particular when they relate to issues of national security, such as government-ordered shutdowns, or the seemingly out of control spread of hate speech on a network. But we now know that companies have provided enlightened leadership in tackling the menace of hate speech. My colleagues at IHRB prepared a study on how a major telecom company in Kenya – Safaricom – played a proactive role to weed out hate speech from SMS – or text messaging – in the run-up to the Kenyan Presidential elections last year. While companies have not collectively challenged government-ordered shutdowns, evidence is emerging of the negative impact of such state imposed requirements, and greater consolidation of efforts is needed to ensure that such shutdowns become rare and time-bound, and only in cases when there’s credible evidence of imminent threat to peace and security.

In order to tackle these challenges and develop long-term stakeholder engagement plans, companies must understand the context in which they operate. Social tensions can shift and spill over quickly, and companies must be prepared to deal with these constructively and consistent with international human rights principles and standards. Over the past few years we have seen Vodafone Egypt learn from its experience during the Arab Spring, where a government ordered shutdown caused a backlash against the company.

As I mentioned, during the 2013 Presidential elections, the Kenyan mobile operator Safaricom put in place measures to mitigate the spread of hate speech via their bulk SMS platform, which had been a trigger of the post-election violence of 2007.
Different companies, different countries, different contexts and challenges can appear overwhelming, and the challenges can indeed at first seem unmanageable. But each company shares the same goal - to provide access to communication and the fulfillment of a range of human rights – to speak, to listen, to gain knowledge, to communicate, to share ideas, to learn, to participate in political processes, to investigate, to care for loved ones, and to feel assured that nobody other than intended recipients of the communications receive the information. It is not too much to ask. It is the rationale – the business model – of ICT companies.

*On-line*

There are robust discussions happening at many fora, from the international gathering that recently concluded in San Francisco – RightsCon - and the Freedom Online Conference, which will take place this year in Estonia, to the Internet Governance Forum in Brazil, and the Stockholm Internet Forum. In these gatherings a wide range of issues are freely discussed. Enlightened companies that aspire to leadership should be part of these dialogues.

Telcos in particular must listen to what consumers want. They want encryption, control over their own data; they want security, safety, privacy, and they want freedom to express themselves. Telcos have now begun to release transparency reports, listing, for example, the number of government requests for user data they receive. Verizon and CREDO are the first companies to do this, with other major European telecommunication companies expected to follow.

5: Where will we be in five years time?

To conclude, let’s look ahead and ask ourselves where will the issue of human rights in the ICT be in five years time? Here’s what I would suggest:

• First, telcos will be increasingly looking at their whole value chain and their intrinsic relationship to the wider ICT sector. No longer are they in silos – of equipment manufacture, builders of telecom towers, enablers of conversations and data transmission, or providers of access. Just as technologies are mingling, so will their role change.

• Second, I believe telcos will remain instrumental in delivering a wide-range of human rights benefits, particularly in developing countries. The growth will be fundamentally different: instead of fixed line, people will switch straight to the cellular; with the rise and ubiquity of smart phones, people will access the Internet through different means, making many earlier technologies obsolete.
The developing world will no longer be the dumping ground for old technologies; the challenge will lie in making hardware and the access to technology cost-effective for consumers whose purchasing power is limited.

• Third, we’ll see the risks as well as the benefits of the sector better and more clearly understood. Greater engagement with stakeholders will help companies refine their perspectives, making them aware of the risks their technologies might pose, even if inadvertently.

• Fourth, the right to privacy will be a central business as well as consumer demand – more and more related products will emerge to help ensure respect for this fundamental right.

• Fifth, supply chains will be more transparent and leverage points will be clearer for common action, at least partly because there will be more stringent procurement criteria from governments, and greater demands from stakeholders, shareholders, regulators, and others, for transparency and reporting of supply chains.

• The future of the Internet will remain uncertain and contested: national security concerns will increasingly dominate but there will be need for greater transparency with the public. People are smart; governments will need to trust them more, and convince them why they need certain data. And if the requests are sensible, societies will agree. Thanks to the revelations of the past year, everyone has seen the future, and nobody wants to wake up on a bright cold day in April when the clock strikes 13.

During the opening ceremony of the London Olympics in 2012, a lone figure sat at a computer in the middle of the vast stadium. As the many cameras zoomed in for a closer look, we learned that the lone figure was Sir Tim Berners Lee, the man widely credited as the inventor of the World Wide Web. As he typed alone at his console, letters 100 feet high were projected onto the audience and travelled around them. He typed, and we read, “This is for everyone”. The Internet must remain for everyone.

The choice is ours – and users, consumers, activists, companies, and governments have to work together to ensure that access to information technologies stay open, where people communicate without fear, and where the people who work do so with dignity.
I hope our discussions today will be a valuable start. Break Out Session One looks at: What would be effective human rights due diligence for DT, especially in the supply chain? That’s the one I am going to: we want to discuss stakeholders’ expectations on effective human rights due diligence with regard to digital rights and the supply chain for DT and to identify the needs of stakeholders as well as of rights-holders and affected groups. Break Out Session Two looks at "Conflict Minerals and challenges and solutions on the way to a responsible sourcing of raw materials" and I know will look at EU and US regulation and further steps to achieve "conflict free" ICT products. Finally, Break Out Session Three looks at “Setting the framework for an improved collaboration on sustainability with our suppliers – what is necessary?”

I wish you all a very productive conference. Thank you.