The Transformative Potential of ICT to Support Human Rights

"Sleeping Giants in the Valley of Opportunity"

Speech delivered at the Global e-Sustainability Initiative (GeSI) meeting
Brussels, 8 May 2018

Keynote speech delivered by John Morrison
CEO, Institute for Human Rights and Business

Thank you to the Global E-Sustainability Initiative for the opportunity to address you this afternoon. I would like to talk about the potential that information and communication technologies provide in strengthening respect for human rights around the world. But I will do so following the maxim that with "power comes responsibility", and reflect on the new responsibilities that are emerging for the industry.

As Professor John Ruggie, former UN special representative on business and human rights, has often said, unlike with carbon in the atmosphere, there is no such thing as "human rights off-setting". The corporate responsibility to respect human rights is, to use another climate-change related idea, an "inconvenient truth". This is why we were pleased to work with the European Commission - and many of your own organisations - back in 2011-2012 to produce its first human rights guidance for the ICT sector – bringing together both off-line and on-line responsibilities within the UN Protect, Respect, Remedy Framework. The concept of human rights due diligence is central to any approach – know your risk and potential negative impacts, do your best to mitigate and prevent them - increasing your leverage where necessary - and provide adequate remedies for victims. This is the UN, EU and OECD standard for business and human rights, which we also now see emerging in national law in some European states.

The valley of opportunity in front of us is indeed fertile and vibrant with colour. ICT is transforming society and transforming efforts to protect human rights. When then US Secretary of State, Hilary Clinton, spoke to the Freedom Online Coalition in Den Haag in 2011, she described the internet as the new frontier in human rights: "...just as we have worked together since the last century to secure these rights in the material world, we must work together in this century to secure them in cyberspace."

In some ways, 2011 seems a long time ago – it was the height of the Arab Spring and there was a different US administration. But in other ways, little has changed - the centrality of the ICT sector to the enjoyment of human rights has only grown. What has darkened the optimism, however, is an acknowledgement of the downside – of widespread surveillance, the easy proliferation of hate speech and fake news, and the growing concern over privacy rights. The underlying and disruptive changes that technology is bringing supersede the political and the here and now. As we approach the 70th Anniversary of the Universal Declaration of Human Rights in December this year, we should remember

the signing of the original document in the Palais de Challiot in Paris in 1948, and reflect on how far Europe has come over the longer term.

The valley of human rights opportunity

As we enter this new valley, despite all the challenges, I am excited by the opportunity. We know that ICT can bolster freedom of expression in ways which have never existed in human history.

Government censors struggle to control social media and when they seek to limit free speech, society responds in new ways, including with memes, images and puns. Think only of China, for example, and the way that "river crabs" now have a whole new meaning, or why Disney's Winnie the Pooh went viral last year, and again wearing a crown the very week President Xi ended term limits for Presidents. China's own social media platforms are indeed more controlled but they too have had positive benefits in helping to identify instances of local corruption and serving as a platform for protests against the environmental degradation of many of China's rivers and urban spaces. ICT has increased the possibilities for dissent, protest and virtual assembly in most places even if governments are fighting back in others, sometimes themselves becoming more sophisticated in using social media to entrap activists, such as in Bahrain for example.

ICT has enabled access to other human rights. Mobile telephone companies have used the infrastructure of 2G and 3G networks to enhance access to information, improve livelihoods, track epidemics, reunite refugee families, educate the rural poor and even provide resources to midwives. Because of these positives, my organisation embedded our researcher within ICT companies in Myanmar, Kenya, Pakistan, and more globally, to better understand how issues such as network shutdowns, proliferation of hate speech, and technologies that enable surveillance pose challenges for private companies, even as universal 3G connectivity brings over-arching human rights potential. Our "digital dangers" programme was a reflection of the ICT industry's human rights power, not its weakness.

Now we look ahead to new wonders. The "Internet of Things" is with us, and so too technologies that can communicate directly with each other and make our lives more convenient and safer. The tsunami that is the Big Data revolution, unleashing more data in one year than has ever existed in history, should deliver knowledge about the world into all our hands. Algorithms will do much of the hard work for us. If you ask if people would trust the algorithms, they already do – take AirBnB or Uber as examples. Millions of people are willing to share their homes and personal possessions, or to get into a stranger's car, guided only by the data generated by other consumers and not the trust in a central institution, with its legions of hotel inspectors or requirements of taxi registration. In London, we have the case of John Worboys, a driver of a traditional London black cab who drugged and raped dozens of female passengers before he was eventually identified and arrested – it is doubtful whether he could have acted with impunity had technology been available to give a voice to all his previous customers.

And finally, the wonder of all wonders, blockchain – a technology that (some say) might even deliver bespoke human rights solutions to some of the older dilemmas around business and human rights – bringing radical transparency, full traceability and much greater responsibility to supply chains. As you might expect, we are looking closely at blockchain this year and what the human rights potential might be.

Three sleeping giants

But as we stroll through the sunlit pastures, we must be aware of the dangers around us. Perhaps a little more hidden, covered in moss and ferns and easily confused with the natural landscape, lie a number of sleeping giants. I would like to identify just three of these giants by name, so we can get to know them a little better before they wake up and knock us down.

<u>Data Privacy</u>

The first of these giants is data privacy. This month the General Data Protection Regulation (GDPR) comes into effect – so you might feel this giant is well and truly awake and roaring. But I would argue that it has yet to really stir. I have been to many events over the years where it was assumed that the right to privacy is only really a matter of concern for celebrities or politicians; that the average person has been willing to trade away a huge part of their online privacy in exchange for the benefits that technology can bring. I have also been told that I am too old to really understand that millennials are much more relaxed about what they share and what is known about them. I would go as far as to say that privacy has been treated with a certain amount of contempt in some policy circles.

GDPR might change this assumption, as I am sure you all know better than I do. Facebook, for example, processes its non-North American data through its Dublin headquarters – so for Facebook, GDPR represents a near-global standard. This is reinforced by Facebook's new user consent form, which is being rolled out globally – with specific requests for users to accept its targeted advertising and to allow features like face recognition. In a recent article in Wired, researcher Michael Veale refers to the Irish data regulator as being weak – until recently it was operating above a supermarket in an office largely staffed by interns. But now this will need to change, and should they want to use it, European data protection agencies will have a lot more power.

Google, which spent years preparing for the new rules, has stopped scanning Gmail messages for keywords used to target advertising. And it recently introduced a new marketing product for publishers that shows ads based on the context of other articles or content on a website, instead of relying on personal information.

Why does privacy matter? The fact that so many politicians trot out the line that those "with nothing to hide have nothing to fear" tells it all – it is an Orwellian quote that is all too often used by those in power with no sense of irony. Research has shown the discriminatory effects of algorithms, how apps for landlords can all too easily discriminate against minority and ethnic communities, or how data-driven policing has become a central concern for the "Black Lives Matter" campaign in the USA. Digital data can also diminish human agency and can be used for social control, in the way that facial recognition technology is being developed to control predominately Muslim populations in Western China. The aggregation of personal data can be a hugely powerful tool – as the Cambridge Analytica scandal revealed.

Perhaps this giant is waking up. If consumers really did start taking an active interest in how their personal data is collected, used and stored – this would have a radical effect on the ICT sector, but also customer loyalty cards in supermarkets or even medical research. Privacy matters – without adequate protections for privacy there can be no creativity, no entrepreneurship, no critical thinking, no accountability, no whistle-blowers, and no human rights defenders. Obviously, a pragmatic balance must be reached between privacy and other priorities, but it is for society to discuss these openly – it cannot be a matter only for unaccountable officials or technologists to decide.

Consent

A recent New York Times article it was said that far from disadvantaging the big players of the industry, the requirement to get consumer consent for every new data use will confer advantages to them in the longer term, even if it represents an administrative headache at present. That is because, as the article argues citing research, consumers are more likely to consent to well-known brands and services to which they are already deeply committed. Having ended my own relationship with Facebook just last month, I can concur this is not an easy thing to do – when so many far-flung family and friends are networked in this way.

This then brings us on to the second of the sleeping giants, a proper understanding of what consent really means. I think we can all agree, there is more to consent than the 40 pages of small print that none of us reads before ticking the consent box online. Consent has to be meaningful and it has to be freely given. The human rights framework provides a solution – the notion of free prior informed consent of FPIC. That idea has been largely understood to apply to cases where land is to be acquired from indigenous communities – and far-thinking companies extend the right to other marginal, vulnerable communities as well. FPIC clearly has applications beyond the land question.

Consent has to be free – free from fear or control. An oil company that conducts consultations with a sceptical community while being protected by armed guards is not conducting the exercise in a free atmosphere. Consent has to be prior – it has to be sought before a specific transaction or activity is to take place. A mining company cannot go to a community and seek its consent after it has begun exploration for minerals. And consent has to be informed – the consenting party should understand the meaning of what is to follow, what the person is giving up and in return of what. People need to know what the pollution effects will be, before they consent to a factory being built near their community.

FPIC is something most companies in the extractive sector, and increasingly, in the manufacturing sector as well, understand. The ICT sector has to see Consent comprehensively, and not as a box-ticking exercise. It may mean differential tariff structures – for example, charging consumers who want greater privacy; informing consumers who want services for free as to what that implies. And being clear, honest, and transparent.

Fake News

The final sleeping giant is the reality of "fake news" and the role of ICT companies in combating it. Governments across the world are increasingly concerned about the widespread proliferation of 'fake news.' If one goes back in history, there has always been fake news. Political rivals have smeared each others' reputations by lying. Others in power have denigrated opponents – including rival businesses, technologies, religions, and ideas – by making stuff up about them. During wars, as the maxim goes, truth is the first casualty, and we use the 'war' metaphor in everything these days – trade wars, culture wars, war of civilisations, and so on. So we have always had fake news.

What has happened, however, is that the Internet is enabling such disinformation and misinformation to spread quickly and widely, reaching more deeply, way before regulators, or the truth, can catch up. Fake news is spread by governments and their opponents. Ukrainians are fighting a conflict with the Russians, and spread of disinformation has swayed many people, forcing the Ukrainian government to ban certain websites and Russian cinema, even though technology enables the mischievous and the malevolent to stay one step ahead of government controls. Governments in the West – the United States in particular – have been criticising 'fake news,' but too often politicians call 'fake news' whatever news they don't like. Governments in a number of countries including Malaysia, the Philippines, Singapore and India, are considering regulatory powers or laws to combat fake news.

Where does an ICT company's responsibility lie? It is inevitable that governments will lean on companies to do the censorship for them – weeding out the fake and keeping the true. But truth is a philosophical concept, and companies are not made up of philosophers. Nor are they made up of lawyers or human rights experts. Companies can try to pass the buck back to the governments, saying it is the state's responsibility – but companies do exercise power to control content, under the omnibus term, 'policies.' Companies will have to reflect on this, think hard, and write policies that are consistent with international human rights standards, and consult far more widely than they do now, so that they make the right decisions. Yes, blocking sites that provide child pornography is illegal, and yes, enabling sale of weapons or contraband drugs is wrong, but preventing views that are controversial (including atheists running rationalist websites, for example), or websites with political satire, are all within normal discourse. Not all companies have the staff that can distinguish between criticism and hate speech, between hate speech and dangerous speech, between a reckless rant on the Internet and actual incitement of violence. They will have to be prepared, skill up, and talk to people beyond their own circles.

Conclusion

So finally, what to do about the three giants, and any others you have discussed yourselves? I very much welcome GeSI's discussions about the positive role technology can play in the realisation of human rights. I know it is a current priority for the UN High Commissioner for Human Rights in the year we celebrate human rights' 70-year birthday party. Technology does support many human rights and new solutions will be found though new and emerging applications, from worker voices in supply chains, data-driven analytics, artificial intelligence all the way to blockchain.

I suppose part of my role today is to remind you that with opportunity comes responsibility. Dealing with issues such as privacy, meaningful consent or fake news will not be easy – no company should work in isolation on such issues. It will be tempting to run past some of these giants, or pretend they are not there. Instead, the industry is better advised, in my opinion at least, to confront them head-on together. I would encourage GeSI and its members to work in wide coalition with many others around the world struggling with the same issues. The world has moved on since we completed the ICT human rights guidance for the European Commission six years ago. We know that guidance alone will not be enough to tackle systemic and complex issues. But collective action – involving civil society, business and governmental agencies – can make a fundamental difference as we have seen in other industries.