Information Technology: The Power and Responsibility of Business

February 2014

Technology is a powerful tool for human rights. Through its reach and influence in all parts of the planet come opportunities for better lives. But information and communications technology (ICT) companies can also be involved in major human rights abuses: either by committing them directly, or by facilitating abuses by governments and other firms. With the ever-increasing scrutiny of companies' conduct – much of this enabled by the internet itself – and the growing availability of practical guidance on how to do the right thing, there is little excuse for inaction.

The Business & Human Rights Resource Centre has been tracking the human rights conduct of companies globally since 2003, including firms in the ICT sector. We highlight positive steps, such as initiatives by mobile phone companies to connect aid with victims in humanitarian disasters, and joint efforts by industry and others to protect freedom of expression and privacy. We also draw attention to allegations of misconduct, for example when companies supply governments with products to monitor human rights activists and disrupt their communications; or when pressures over price mean workers in technology supply chains work excessive hours, in harmful conditions, for very low pay.

From **Apple**, to **Nokia**, to **ZTE**, we have invited ITC firms to respond to specific human rights allegations raised by civil society organizations over 220 times, with a response rate of 70% (full details of all these approaches are here). The quality of companies' responses varies, yet this has proved to be an effective tool for transparency, engagement, and public accountability. It also enables differentiation between those that are taking a leadership stance on human rights from those that are obstructing progress. In 2005-6, four percent of the companies we invited to respond to concerns were from the ICT sector – by 2012-13, this figure increased to thirteen percent, demonstrating the increasing attention on the sector.

Below we highlight key cases and lessons from our work. We draw from situations that we and other human rights organizations have worked on in six areas:

- **Combating censorship**
- **Curbing surveillance and repression**
- **Protecting privacy**
- **Broadening access**
- **Engaging the supply chain**
- **Respecting children's rights**

Navigating the human rights dimensions of ICT is fraught with challenges, for civil society groups and for companies alike. We fully recognize that, and hope that this briefing provides some clarity on the subject as well as pointers to pitfalls and opportunities. The briefing wraps up with recommendations for companies and for governments.

Combatting censorship

In February 2012 the Pakistan Government issued a tender for a "National Level URL Filtering and Blocking System." This system would enable the government to inspect and track all internet traffic in the country, and deny access to websites based on a number of factors, including a blacklist of certain sites as well as banned keywords. The Pakistan-based human rights organization Bolo Bhi raised the alarm and called on ICT companies *not* to bid. We worked with them to approach the companies: **Cisco, McAfee, Sandvine, Verizon** and **Websense** all committed publicly not to bid for the tender – with the latter also calling on other companies to do the same. However in June 2013, Citizen Lab, at the Munk School of Global Affairs at the University of Toronto, reported that technology from the Canadian firm **Netsweeper** was being implemented in Pakistan "for the purposes of political and social filtering."

As Shahzad Ahmad of the Pakistani human rights group Bytes For All said in a *Toronto Star article*: *"We have just gone through the first ever democratic transition to a new government that won power through the vote…No company, from Canada or anywhere, should be helping the government introduce a kill switch on information."* Netsweeper, which had not responded to the initial call, also declined to respond to these new findings. So we wrote to the Canadian government. We asked what steps it was taking to urge Netsweeper to respond publicly to these concerns – bearing in mind the duties of the Canadian Government and the responsibilities of Netsweeper, under the UN Guiding Principles on Business and Human Rights.

In its reply, the government cited its commitments to human rights and to promoting corporate responsibility. It also referred to the government's membership in the Freedom Online Coalition, a group of governments working to protect human rights online. But it added, "we cannot speak about the affairs of any one firm due to privacy constraints." David Petrasek of the University of Ottawa commented: *"The silence of the Canadian government in this case is shameful, and provides a cover for companies to ignore human rights concerns. For if the government refuses to comment, or even to note that it has expressed its concern, it implicitly legitimizes the insouciance of company officials."*

Another company that declined to respond about censorship concerns was **Orange**. Journalists and human rights activists in Jordan held a protest outside its headquarters in Amman in June 2013. As the main internet provider in the country, they alleged that it had helped stifle freedom of expression by complying with a temporary government shut-down of nearly 300 online news websites. Police dispersed the protestors using batons and tear gas. The editor of one of the sites, Jo24, said: *"Orange company is helping the government violate the constitution, which grants freedom of expression. Journalists are determined to make their voices heard no matter what."* The Resource Centre invited Orange to respond to this, and its reply was *"Nous ne souhaitons pas faire de commentaire sur ce sujet,"* i.e., *"We do not wish to respond on this matter".*

In India, where the government is, according to the Committee to Protect Journalists, pursuing a "perilous trajectory" on internet freedom, international companies have been pushing back. **Google** and **Facebook**, for example, have challenged through the courts a lawsuit brought against them for allegedly hosting "offensive content". Google is also challenging charges brought against it by construction materials company Visaka Industries, which alleged an activist spread false information about Visaka on Google's blogging platform Blogger. In Pakistan (where Google does not have a physical presence, unlike India), the company's resistance to a government request to censor the "Innocence of Muslims" movie trailer has led to an outright ban on YouTube in Pakistan (YouTube is owned by Google). Human rights activists in the country are campaigning for the ban to be lifted and are challenging it in the courts.

These cases demonstrate the shifting line between government and corporate influence in the realm of internet freedom. It shifts according to the government's stance, the legal status of a company in a particular country, and the company's own decision-making. As Rebecca MacKinnon, Director of Ranking Digital Rights and author of *Consent of the Networked* comments in a recent article in Guernica magazine, "*Commercial sovereigns like YouTube's parent company, Google, are the new arbiters—sometimes censors, sometimes champions—of a large and growing percentage of citizen speech all over the world."* Yet at the same time they are not free from government controls, of course. She adds: *"If a company were to commit to decline all government censorship or surveillance requests, it would be able to do business precisely nowhere."* Companies that take human rights seriously identify ways to minimize their complicity in government censorship and other abuses, and to apply their policies consistently throughout their operations.

Curbing surveillance and repression

Many human rights activists rely heavily on communications technology. It helps them to get the word out about human rights abuses, to connect with each other, and to mobilize both online and on the streets. However it can also be used against them, when ITC firms' products – with or without the knowledge of the firms – are used by governments to target them. As Privacy International has said in the context of its "Big Brother Inc" project that strengthens transparency and accountability in this area: *"The global surveillance industry is estimated at $5 billion a year. The capabilities of surveillance technology have grown hugely in the past decade – in the hands of a repressive regime, this equipment eradicates free speech, quashes dissent and places dissidents at the mercy of ruling powers as effectively as guns and bombs, if not more so."*

In February 2013, Privacy International, the European Center for Constitutional and Human Rights, Bahrain Watch, the Bahrain Center for Human Rights and Reporters Without Borders filed an OECD Guidelines complaint against **Gamma International** (based in the UK and Germany), and **Trovicor** (based in Germany). The complaint called on the relevant National Contact Points (NCPs) for the Guidelines to ascertain whether the firms breached eleven of the Guidelines by exporting surveillance technology to Bahrain, where it was allegedly used to target human rights activists. The firms' spyware installs itself on targets' computers where it can relay information about their activities back to the sender, including the contents of emails and Skype calls.

In June 2013, the UK Government's National Contact Point for the OECD Guidelines accepted the complaint against Gamma for further investigation. The German National Contact Point rejected many elements of the complaint against Trovicor, saying they would only accept it for further investigation of Trovicor's due diligence proceedings – following which the NGOs withdrew the complaint. Privacy International's Head of Research Eric King said: *"The NCP's unwillingness to examine Trovicor's role in human rights abuses in Bahrain is shameful. By failing to investigate the extent of the company's wrongdoing, the NCP is turning a blind eye to how German made surveillance technology is being used by the Bahraini government to target and suppress pro-democracy voices."*

In a September 2013 response that Trovicor sent us about this issue, it describes its decision-making process for deciding whether to supply a country or customer, and says that it "doesn't supply any country which is in civil war or in conditions similar to civil war or for which such conditions are predictable." It also adds: *"Please understand that our contractual terms don't allow us to comment on individual clients, nor can we publish the countries that Trovicor does not trade with."* Gamma has said in the media that it had not sold its product to Bahrain and that the programmes used there may have been stolen.

Companies allegedly involved in enabling government repression expose themselves to legal risk. In 2011, five Libyans who were tortured under Moamer Gaddafi filed a lawsuit in France against the French technology company **Amesys**. They allege that the company provided the Libyan government with communication surveillance equipment which was used to identify them as Gaddafi opponents, which led to their detention and torture. Amesys has confirmed that it entered into an agreement with Libyan authorities in 2007 but claims that the equipment provided did not enable the monitoring of telephone lines. It says that its activities comply with international, European and French law. In January 2013, an appeals court approved a judicial inquiry into allegations of Amesys's complicity in acts of torture to proceed. We have a profile of this case on our "Corporate Legal Accountability Portal", which includes a summary of the case and relevant materials related to the legal proceedings. As Michael Smyth, a former partner at Clifford Chance law firm says in commentary provided for our Corporate Legal Accountability Portal: *"There was a time when business layers did not need to know a great deal about human rights law. That is no longer the case."*

A well-reported case is that of **Yahoo!** in China and the journalist Shi Tao. Back in 2005, the company complied with Chinese government requests for Shi Tao's account information, which led to his arrest and detention. At the time, Yahoo!'s response was*: "Just like any other global company, Yahoo! must ensure that its local country sites must operate within the laws, regulations and customs of the country in which they are based."* Human rights experts critiqued this response. For example, Mary Robinson, former UN High Commissioner for Human Rights and President of Ireland, said: *"I was shocked and dismayed by Yahoo's response…It appears that Yahoo is unaware of growing public expectations that businesses must assume their appropriate responsibilities for the promotion and protection of international human rights standards wherever they operate. In the time ahead, Yahoo needs to give careful consideration to its role in fostering greater respect for human rights around the world…"*

Yahoo! embarked on a steep learning curve, and is now among the companies taking a strong stance on human rights. It was a founding participant in the Global Network Initiative, a multi-stakeholder initiative that aims to protect and advance freedom of expression and privacy in ICT companies (other corporate participants are **Evoca, Facebook, Google, Microsoft, Procera Networks and Websense**) It has a dedicated Business and Human Rights Program and has committed to conducting human rights impact assessments for its business decisions. And it is sharing its experience with other firms, for example it recently convened a meeting for tech start-ups to educate them about challenges to privacy and free speech that they will inevitably face.

Another firm that has conducted an internal learning process on human rights is Kenya's largest mobile network provider, **Safaricom**. The 2007 Presidential election in Kenya led to an outbreak of post-election violence that left over 1,000 people dead and over 600,000 displaced. SMS messages and blogs were found to have fuelled the violence by exploiting tensions between ethnic communities. In the run-up to the 2013 elections, Safaricom devised a code of conduct and system to prevent spreading hate-filled messages through its bulk SMS service. The Institute of Human Rights and Business, whose "Digital Dangers" project examines how ITC companies are handling human rights challenges has produced a detailed case study of Safaricom's actions to address the issue of hate speech.

Respecting privacy

The revelations by Edward Snowden of the US Government's "PRISM" programme highlighted the extent to which the privacy of technology users can be violated without their knowledge. Under the programme, the National Security Administration obtained private user data from technology companies on a widespread scale. Major ITC companies' responses included a combination of

denying knowledge of the PRISM programme, clarifying their own positions, and challenging the US government. Some filed lawsuits against the US government calling on it to allow them to release information on government requests for user information. In December 2013 a group of companies launched a joint initiative called "Reform Government Surveillance", saying that they *"believe that it is time for the world's governments to address the practices and laws regulating government surveillance of individuals and access to their information."* Signatories are **AOL, Apple, Dropbox, Facebook, Google, LinkedIn, Microsoft, Twitter** and **Yahoo!** In January 2014, the Justice Department relaxed some of the rules allowing companies to disclose some information about government requests for user data – firms welcomed the move but many will continue to push for further changes.

Among other organizations, the Institute for Human Rights & Business (IHRB) is examining transparency reports by companies over government requests. As IHRB researcher Lucy Purdon has highlighted, the clarity of the reports and the way they are used will be key*: "It is encouraging to see companies building on each other's work by releasing their own transparency reports and that each report becomes a little more transparent than the last…but it is important to see beyond the tables and graphs and remember that there are people attached to the numbers…and when governments act [on user information received from companies], there can be negative human rights consequences."*

Some level of government surveillance is required for security purposes, of course, but civil society organizations have emphasised that it is important that surveillance activities online be justified as necessary, and proportionate to the threats in question. As Citizen Lab Director Ron Deibert has said, *"For me it's not really about privacy ... it's about the potential for the abuse of unchecked power."* An additional consequence of the revelations of the US Government's PRISM programme is that it provides other governments with additional "justification" for similar programmes.

Broadening access

Around sixty percent of the world's population is still not online. Expanding access to technology and telecoms is in itself an important contribution to human rights: not only does it enable freedom of information and expression, but it can help empower marginalized groups, fuel development and combat corruption.

It is also an essential tool for organizations working on business and human rights. To take two examples just from Cambodia: Open Development Cambodia provides maps of land concessions and the companies involved; and Sithi.org, a project of the Cambodia Center for Human Rights, has a map of over 500 garment factories, providing the factories' names, major buyers, and number of workers. Transparency initiatives such as these can push companies to improve their conduct in the knowledge that they are under scrutiny, and also equip activists and the public at large with information needed to hold companies accountable. Our own organization, Business & Human Rights Resource Centre, could not exist without the internet: a core part of our work is providing an online information hub that enables greater transparency, accountability and access to guidance on companies' human rights impacts worldwide.

Many companies are already taking powerful steps to bring ITC to a broader global audience. Recently, for example, Unilever has partnered with the Facebook-led alliance Internet.org to understand how internet access can be increased to reach millions more people across rural India – currently just 13 per cent of the Indian population has internet access. The partnership will draw on Unilever's experience reaching rural communities in India. Internet.org is a "global partnership between technology leaders, nonprofits, local communities and experts who are working together to

bring the internet to the two thirds of the world's population that doesn't have it." Its founding partners are **Ericsson**, **Facebook**, **Mediatek**, **Nokia**, **Opera**, **Qualcomm** and **Samsung**.

Given the enabling power of technology, companies have an important role to play in expanding access to their products, and also therefore in resisting efforts to cut off access. It was well-reported that during the protests in Egypt that lead to the overthrow of Mubarak, an internet service blackout took place. Human Rights First wrote to telecommunications and internet providers operating in Egypt, asking them to be transparent about government requests to interrupt communications services, how they made decisions about responding to such requests, and what the company's official policies are on communicating those decisions to the public.

We approached the companies for public responses. **Etisalat** and **Telecom Egypt** did not respond, but **LINKdotNet, Noor Group** and **Vodafone** did. In its response, for example, Vodafone described the sequence of events (involving the blackout and also pro-Mubarak propaganda text messages that the authorities requested the telcos to send to users), and stated: *"At all times during the crisis situation Vodafone's decisions were based on how it could best balance the needs and safety of its employees on the ground in Egypt, its customers and the broader population of Egypt."* Vodafone is one of the participants in the Telecommunications Industry Dialogue, a group of telecommunications companies addressing freedom of expression and privacy rights in line with the UN Guiding Principles on Business and Human Rights. Other participating companies are **Alcatel-Lucent, At&T, Millicom, NSN, Orange, Telefónica, Telenor** and **Teliasonera**.

As Electronic Frontier Foundation has highlighted, internet shut-downs have been on the increase since 2011. For example, in Sudan, internet services were abruptly shut down on 25 September 2013, on the third day of protests in Khartoum over the cutting of fuel subsidies, which had doubled the price of gas. The digital rights NGO Access called on the companies that provide networks in Sudan to report on their activities relating to the shutdown, and we also reached out to them for a response – Zain; CanarTelecom, MTN and Sudani/Sudatel. In its response, **MTN** said: "*Following the internet outage in Sudan, the National Telecommunications Corporation (NTC) indicated that the interruptions were 'due to sabotage of Canartel's servers and equipment'. Canartel is MTN Sudan's internet service provider, and therefore MTN was unable to immediately address the cause of the shutdown. However, with the assistance of Canartel, MTN was able to resume services within 15 hours of the shutdown. We are in on-going discussions with Access, and have incorporated various recommendations from their Telco Action Plan into our Human Rights policy."*

In another case, Bloomberg BusinessWeek reported that in Somalia in January 2014 **Hormuud**, the Somali-based telecoms company, shut down its internet and email data service in response to a threat from the extremist group Al-Shabab, which gave phone companies a deadline to close down services over fears that the US government can tap into data and target militants.

Access has published a guide called "Forgotten Pillar: The Telco Remedy Plan", which *"assists companies to implement both the procedural aspects of remedy, such as safe and accessible grievance mechanisms, and the substantive aspects, which may be as simple as an explanation and commitment to non-repetition. By approaching the question of remedy holistically, throughout the entire human rights due diligence process, telcos will be prepared to address those affected in a more timely and cost-effective way."* Access also provides guidance more broadly on human rights issues for telecom companies in its "Telco Action Plan – Respecting Human Rights: Ten Steps and Implementation Objectives for Telecommunications Companies."

As countries expand their internet and telecoms network it is important that the relevant privacy and freedom of expression safeguards are in place. Myanmar (Burma) is currently dealing with many of these challenges. In January this year, 61 civil society organizations wrote to the World Bank raising concerns with its Telecom Sector Reform Project for the country. They highlighted the fact that

"Burma has unique potential to leapfrog its neighbors in telecom development and to implement a regulatory framework that meets international human rights standards." Human Rights Watch (HRW) has called on the two telecoms companies that have won licenses to expand telecommunications in Myanmar, **Telenor** of Norway and **Ooredoo** of Qatar, to "make a public commitment to strong human rights policies and broad transparency measures". As HRW's senior internet researcher Cynthia Wong said: *"Burma's long record of rights abuses should give pause to the two license winners about government censorship, illegal surveillance, and even network shutdowns. The firms should put strong safeguards in place for their users, make clear that they will be transparent about government demands, and press the government to enact legal protections for rights."* Telenor and Ooredoo have responded, setting out their human rights commitments in this context.

Engaging the supply chain

Several of our approaches inviting ITC companies to respond to human rights-related concerns have been over impacts in their supply chains. This includes the sourcing of "conflict minerals" from the Democratic Republic of Congo – the revenue from which supports local militias who carry out abuses including beatings, rape, and other forms of violence. **General Electric, Microsoft and Motorola** are three companies that distanced themselves from the American Chamber of Commerce efforts to stymie the effective implementation of provisions in the US "Dodd Frank Act" aimed at curbing this issue through disclosure and due diligence requirements: prompting Global Witness to call on other companies to follow suit. Various companies have now started to implement this provision as the first disclosure reports are due in May 2014. **Apple** and **Intel** are examples of other companies taking a principled stand on conflict minerals, working to achieve a "conflict-free" supply chain.

We have highlighted reports and obtained company responses over alleged abuses of workers' rights in mobile phone factories in China (for example at **Foxconn**, a major supplier of **Apple**). In China, we also helped a coalition of environmental NGOs led by the prominent Chinese environmentalist Ma Jun to engage more technology firms in reducing widespread water pollution by their supply factories, where it posed a serious threat to local residents' health. Ma Jun made a compelling presentation about achievements and challenges of this work, as the keynote speaker at the second event in our annual Mary Robinson Speaker Series on Business and Human Rights, in New York City in 2011.

Respecting children's rights

ITC companies are often expected to have additional protections in place for children. In February 2012, the UN Committee on the Rights of the child released the "General Comment on State obligations regarding the impact of businesses on children's rights." Among many areas, it states that *"Digital media is of particular concern, as many children can be users of the Internet but also become victims of violence such as cyber-bullying, cyber-grooming, trafficking or sexual abuse and exploitation through the Internet…States…should coordinate with the information and communication technology industry so that it develops and puts in place adequate measures to protect children from violent and inappropriate material."* In one example of action in this area, in the UK, **Google** and **Microsoft** agreed in November 2013 to block 100,000 "unambiguous" search terms directing people to illegal child abuse-related content – though campaigners also cautioned that pedophiles are likely to use more obscure search techniques to find content.

The International Telecommunications Union and UNICEF are currently developing Guidelines for Industry on Child Online Protection.

Striking the right balance between protecting children and ensuring freedom of expression can be challenging. And as Human Rights First has pointed out: *"All governments struggle to balance a*

need to deal with serious issues such as security, hate speech, and child safety for their citizens but in repressive societies, these concerns often serve as convenient pretext to engage in censorship or surveillance of the Internet that violates the rights and privacy of users and threatens the free flow of information."

Guidance and recommendations

Recommendations for companies

Human rights provide protection against abuses of power. As the influence of the private sector over people's lives has grown, attention to its human rights responsibilities has also increased. ITC companies that do not take human rights seriously face increasing reputational, legal and financial risk.

There is a growing amount of practical guidance for ITC companies that want to make sure their activities help further, rather than restrict human rights. **This page** of our "Tools & Guidance" portal provides links to the key guides available for technology firms. The many tools available include:

- "ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights", by Shift and IHRB, commissioned by the EU
- Microsoft's "How Microsoft Did It: Implementing the Guiding Principles on Business and Human Rights";
- The "Privacy" dilemma-discussion for companies, on the Business and Human Rights Dilemmas Forum (a joint initiative of UN Global Compact and Maplecroft)
- "Human Rights and Technology Sales: How Corporations Can Avoid Assisting Repressive Regimes," by Electronic Frontier Foundation.

As a starting point, below are principles for action by ITC companies. They are applicable across the areas highlighted above, i.e.: Combatting censorship; Curbing surveillance and repression; Respecting privacy; Broadening access; Engaging the supply chain; Respecting children's rights. We have grouped them under the three principles that drive our own work on business & human rights: *transparency; accountability; and empowering others to act.*

Transparency

Human Rights Statement: Ensure the company has a publicly-available human rights policy statement, citing international standards (including the UN Guiding Principles and relevant sustainability goals), and signed off at board level. This is the "springboard" for action throughout the firm on human rights.

Report on Action and Impact: Deliver thorough, non-financial reporting on human rights promotion, impact, and challenges. Report to the greatest extent possible on government requests for user-data.

Accountability

Ensure the human rights statement is followed through in practice, in the following ways:

Assess Impact: Conduct a detailed impact assessment to identify human rights risks in areas encompassing (but not limited to): freedom of expression; potential complicity in human rights abuses by governments; privacy; labour rights in the supply chain and direct operations; conflict minerals in the supply chain; product use.

Manage Human Rights Respect and Risks: On the basis of the impact assessment, establish clear processes and responsibilities within the company for preventing human rights abuses (indirect or direct), and also for responding to and mitigating them when they do occur.

Train Employees on Human Rights Risks: Provide regular comprehensive and tailored training to employees on human rights risks relevant to the company's activities and to employees' specific responsibilities (for example supply chain management, data handling, government relations, human resources, etc).

Remedy Human Rights Abuse: Whatever preventative measures are in place, it is likely that any ITC company will find itself faced with situations in which human rights are at risk – sometimes leading to abuses. Steps are needed to ensure complaints mechanisms, and remedy for these abuses. The UN Guiding Principles state that to be effective, 'non-judicial' remedies need to be: "*legitimate; accessible; predictable; equitable; transparent; rights-compatible; and a source of continuous learning."*

Empowerment

Constantly explore and support ways in which access to technology can be a force for human rights. The immense power and reach of many ITC companies means they also have enormous potential to actively promote empowerment and participation of citizens through access to communications tools, openness in both government and business, connectivity between users, and support for human rights defenders. Also, take steps to challenge government requests to cut off access, particularly in times of political unrest and protest.

Engage with Stakeholders: There are many ways in which companies need to be openly interacting with partners, stakeholders and critics on human rights issues. This might include participating in multi-stakeholder initiatives such as the Global Network Initiative; engaging with non-profits working on issues such as freedom of expression and privacy; pushing governments to be more proactive on human rights and technology; and participating in government-led initiatives such as the Freedom Online Coalition and the Stockholm Internet Forum.

Recommendations for governments

As the cases in this briefing have made clear, governments play an essential role in technology companies' contribution to and infringements of human rights. Often there is a disconnect between the international reach of technology and of companies that provide it, and the confines of national laws. Therefore in this area, as in other areas of human rights, international law provides a powerful reference point to guide government action and to push repressive governments to change. Below are examples of key documents, relevant to this context, which draw their inspiration from international human rights law and/or standards:

1. The UN Guiding Principles on Business and Human Rights, adopted by consensus by all governments on the UN Human Rights Council in 2011, rest on three 'pillars', the first of which is the "State Duty to Protect" (the other two are the "Corporate Responsibility to Respect, and Access to Remedy). Excerpt: *"States must protect against human rights abuse within their territory and/or jurisdiction by third parties, including business enterprises. This requires taking appropriate steps to prevent, investigate, punish and redress such abuse through effective policies, legislation, regulations and adjudication."*

2. "Necessary and Proportionate": These "International Principles on the Application of Human Rights to Communications Surveillance" currently have over 450 signatories, from civil society and academia. Excerpt (from the Preamble): *"Activities that restrict the right to privacy, including communications surveillance, can only be justified when they are prescribed by law, they are necessary to achieve a legitimate aim, and are proportionate to the aim pursued."*

3. "Reform Government Surveillance": is a joint call on governments by a group of information technology companies that calls for action in five areas: "Limiting Governments' Authority to Collect Users' Information"; "Oversight and Accountability"; "Transparency About Government Demands"; "Respecting the Free Flow of Information"; and "Avoiding Conflicts Among Governments." (signatories are AOL, Facebook, Google, LinkedIn, Microsoft, Twitter, Yahoo).

4. The UN General Assembly adopted a resolution in 2013 called "The Right to Privacy in the Digital Age." Electronic Frontier Foundation hailed it: "One Small Step for Privacy, One Giant Leap Against Surveillance." Excerpt: The resolution calls upon all States *"To respect and protect the right to privacy, including in the context of digital communication",* and *"To take measures to put an end to violations of those rights and to create the conditions to prevent such violations, including by ensuring that relevant national legislation complies with their obligations under international human rights law".*

5. The UN General Comment no. 16 developed by the Committee on the Rights of the Child expressly details "State obligations regarding the impact of the business sector on children's rights." Excerpt*: "…States should…coordinate with the information and communication technology industry so that it develops and puts in place adequate measures to protect children from violent and inappropriate material."*

Follow-up and contact

We welcome suggestions of cases and initiatives – from civil society, companies and governments alike – to feature on our website, and in our Weekly Update emails sent to over 18,000 people worldwide. Given the breadth of this issue, and also the fact that new challenges and opportunities arise all the time, this briefing is not comprehensive, but highlights key cases as illustrations of key issues.

Contact: Annabel Short, Program Director, short@business-humanrights.org / +1 212 564 9160.

Contact details for all of our global team are on our website. We currently have researchers based in Colombia, India, Kenya, Lebanon, Myanmar, Senegal, South Africa, UK, Ukraine, USA.

To keep track of updates, please consider signing up for our free Weekly Updates, and checking the "Technology, telecoms & electronics" and "Internet companies" sections of our site (both with RSS feeds).

Business & Human Rights Resource Centre is an international non-profit organization that encourages companies to respect and promote human rights, and avoid harm to people. It does this by advancing transparency and public accountability, and by empowering others to act. More at www.business-humanrights.org/Aboutus.