OECD Global Forum on Responsible Business Conduct

Report of the Special Event on Responsible Business Conduct in the ICT Sector

Multinational Enterprises, Human Rights and Internet Freedom
27 June 2013, OECD Conference Centre, Paris
14.30-16.00

Contents

1. Executive Summary

The Institute for Human Rights and Business (IHRB) and the Norwegian National Contact Point (NCP) hosted a special event at the OECD Global Forum on Responsible Business Conduct in Paris to discuss the application of the updated OECD[1] Guidelines for Multinational Enterprises ("the OECD Guidelines")[2] to the Information and Communication Technology (ICT) Sector.

[1] The Organisation for Economic Cooperative Development (OECD)

[2] http://www.oecd.org/daf/inv/mne/oecdguidelinesformultinationalenterprises.htm

The 2011 updated OECD Guidelines recognise the importance of the Internet in enabling the enjoyment of a range of human rights. The Internet has a dual existence within the context of the OECD Guidelines: one, ICT is a significant business sector that has responsibilities under the OECD Guidelines, both in terms of impacts of companies' "off-line" relationships (e.g. manufacturing equipment that is often done through supply chain relationships) as well as their "on-line" impacts (e.g. the impact on freedom of expression and privacy). Two, Paragraph IIB1 of the Guidelines expresses the "need to support, as appropriate to their circumstances, cooperative efforts in the appropriate fora to promote Internet freedom through the respect of freedom of expression, assembly and association online".

The purpose of the June 2013 session was to deepen understanding between governments, companies, civil society and trade unions of the relevance of the OECD Guidelines in relation to the ICT sector, with particular reference to human rights and Internet freedom. IHRB and Shift[3] recently developed the *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights* for the European Commission[4], aimed at the broad spectrum of ICT companies, from manufacturing companies in the supply chain to companies offering web-based services. It is hoped this Guide will assist NCPs in understanding the human rights challenges and prompting the appropriate level of due diligence in the sector.

Two important recent events that impact the ICT sector meant discussions at the session expanded beyond "Internet freedom" to encompass a broader debate on the impact of the sector on human rights, in particular the impact of surveillance technology and its application. Perhaps inevitably, a common thread running through both panels was the recent allegations of mass surveillance by governments on citizens' communications in light of leaked documents published in The Guardian[5] and Washington Post[6] newspapers. In addition, in January 2013, NCPs received their first complaint[7] regarding the impacts of two ICT companies selling surveillance technology to the government of Bahrain on freedom of expression and privacy and a possible violation of the OECD Guidelines.

The session consisted of two panel discussions. The first concentrated on the realisation of Paragraph IIB1 of the OECD Guidelines, exploring existing co-operative efforts in the ICT sector to promote Internet freedom and respect for freedom of expression, association and assembly online. ICT companies are increasingly becoming involved in multi-stakeholder and industry initiatives in order to act together and create a level playing field in terms of respecting human rights. Participants discussed the importance of collaboration and ensuring that efforts were not duplicated across the sector.

Participants often referenced the recent revelations alleging government mass surveillance practices and discussed the next steps for companies in addressing such requests from governments and how collaborative industry efforts could consolidate these next steps. It was clear from the discussions that business, government and civil society are still evaluating the implications of these developments for their own work and how to move forward, but it was generally agreed that further transparency around government requests for user data is paramount and that companies must push for this to the fullest extent possible.

[3] http://www.shiftproject.org/publication/european-commission-ict-sector-guide

[4]http://www.ihrb.org/pdf/eu-sector-guidance/EC-Guides/ICT/EC-Guide_ICT.pdf

[5] http://www.guardian.co.uk/world/the-nsa-files

[6] http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

[7] https://www.privacyinternational.org/sites/privacyinternational.org/files/downloads/press-releases/jr_bundle_part_2_of_2.pdf

The second panel focused on the role of NCPs and the recent complaints filed regarding the sale of surveillance technology to the government of Bahrain. The ICT sector is a new area for many NCPs, and participants discussed upcoming challenges NCPs may face as well as how the NCP mediation process has particular significance for the ICT sector. Investors and Export Credit Agencies (ECAs) are increasingly looking to final statements from NCPs for guidance on which companies they should avoid for investment. This could have significant impacts for ICT companies if they refuse to engage with NCP mediation processes as ECAs often underwrite the sale of particular technology.

Apart from the two recently filed complaints on the surveillance sector, there are no other NCP cases referring to the ICT sector, especially regarding privacy, freedom of expression, assembly and association online. Therefore the discussion concentrated on the current NCP complaint regarding the sale of surveillance technology to the government of Bahrain and other possible areas of complaints NCPs can expect to see in the future, as well as possible remedies.

Main areas of discussion:

- **The role of multi-stakeholder initiatives in the ICT sector promoting Internet freedom, freedom of expression, assembly and association online.**
- **Challenges for the ICT sector associated with mass surveillance revelations.**
- **The importance of transparency concerning government requests for access to networks and data.**
- **Challenges for NCPs in addressing issues in the ICT sector, given that the sector involves new human rights issues that NCPs previously have not addressed.**
- **Addressing the first ICT complaint to an NCP relating to surveillance technology and developing possible remedies.**
- **Shaping robust NCP responses in the ICT sector.**

2. Background

The session on the ICT sector was held in Paris on 27 June 2013 during the OECD Forum on Responsible Business Conduct. It was facilitated by IHRB and the Norwegian NCP under the Chatham House rule of non-attribution.[8] Participants included OECD representatives, business and civil society[9].

The OECD Guidelines currently apply in 44 adhering countries: [10] 34 are current OECD members[11] and in addition, Argentina, Brazil, Colombia, Egypt, Latvia, Lithuania, Morocco,

[8] As such, this report does not attribute specific comments to any individuals. Specific references are made in this report when information was presented formally in the panels and is derived from publically available material.

[9] This was the first meeting IHRB and the Norwegian NCP have hosted on the ICT sector, following a previous joint meeting in March 2012 on the extractive sector. http://www.ihrb.org/pdf/IHRB-NNCP-OECD-National-Contact-Points-and-the-Extractive-Sector-FINAL.pdf
IHRB hosted a follow up meeting on extractives in March 2013 jointly with the UK Department for Business, Innovation and Skills. http://www.ihrb.org/pdf/IHRB-NNCP-OECD-National-Contact-Points-and-the-Extractive-Sector_2013-Update.pdf

[10] OECD Annual Report on the OECD Guidelines for Multinational Enterprises 2012: Mediation and Consensus Building. OECD Publishing, Paris, 2012.

[11] The OECD member countries are: Australia, Austria, Belgium, Canada, Chile, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain, Sweden,

Peru, Romania and Tunisia also adhere to the Guidelines. Two additional applications from Costa Rica and Jordan are being processed and the Russian Federation is on an accession path to becoming an OECD member.

The ICT sector is one of the fastest growing sectors and the Internet and digital communications have become a valuable tool in fostering greater enjoyment of many human rights. 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. Due to the fast-paced nature of technology, ICT companies are facing increasing challenges in fulfilling the corporate responsibility to respect human rights. For example, many governments, formally and informally request that ICT companies impose surveillance on individuals or groups, or to permit governments to intercept their communication; to block specific websites; to seek access to data to gather intelligence; and on occasion, to suspend access to the Internet and mobile phone networks, citing reasons of national security or public order, with or without judicial oversight.

In January 2013, the first complaint regarding the ICT sector was filed against two companies with the UK and German NCPs for violation of the OECD Guidelines with regard to the sale of surveillance technology to Bahrain where it is alleged the technology was used in violating human rights.[12] The complaint has so far been accepted by the UK NCP and will go to NCP mediation. Due to the rapid expansion and fast-paced nature of the ICT sector, it is likely that NCPs can expect to receive more complaints regarding the use of technology. The event was therefore timely, allowing a focused discussion of the issues.

2.1 Agenda of the Sessions[13]

Panel 1: Cooperative Efforts to Promote Internet Freedom

Following introductory remarks by the session chair, John Morrison, Executive Director of the Institute for Human Rights and Business, representatives of three multi-stakeholder and industry initiatives in the ICT sector gave short presentations. John Kampfner represented the Global Network Initiative (GNI).[14] Christine Diamente represented the Telecommunications Industry Dialogue on Freedom of Expression and Privacy (the Industry Dialogue), recently housed under the auspices of the GNI.[15] Marie Baumgarts spoke on behalf of the Global E-sustainability Initiative (GeSI).[16]

Panel 2: OECD National Contact Points and Interpreting the OECD Guidelines in Relation to the ICT Sector- Why It Matters

The discussions were opened with reflections from Eric King, Head of Research at Privacy International[17], Laura Ceresna, Policy Advisor at CIVIDEP[18] and Roel Nieuwenkamp from the

Switzerland, Turkey, the United Kingdom and the United States.

[12]https://www.privacyinternational.org/sites/privacyinternational.org/files/downloads/press-releases/jr_bundle_part_2_of_2.pdf

[13] See Annex I

[14] www.globalnetworkinitiative.org

[15] http://www.globalnetworkinitiative.org/news/key-telecommunications-players-collaborate-global-network-initiative-freedom-expression-and

[16] www.gesi.org

[17] www.privacyinternational.org

[18] www.cividep.org

Foreign Ministry of the Government of the Netherlands. The panel was chaired by Margaret Wachenfeld, Director of Legal Affairs at the Institute for Human Rights and Business.

3. Main Areas of Discussion

3.1 Multi-Stakeholder Initiatives in the ICT Sector Promoting Internet Freedom, Freedom of Expression, Assembly and Association Online

- The revised OECD Guidelines encourage co-operative efforts to promote Internet freedom through respect of freedom of expression, assembly and association online. The ICT Sector has several co-operative efforts in the form of multi-stakeholder and industry initiatives (MSIs) which strive to do just that. One panellist stressed there is no "silver bullet" to address the challenges companies face in terms of respecting human rights in the ICT sector, therefore multi-stakeholder initiatives (MSIs) play an important role in encouraging companies to work together and reach out to different members in order to create a "level playing field".

- The question was raised as to whether there are too many MSIs in the ICT sector and given the number, is there collaboration across the different initiatives? One participant argued that there is value in having different models and stressed collaboration across MSIs is important and does take place in the ICT sector. For example the Industry Dialogue is now housed under the auspices of the Global Network Initiative and is working with GeSI.

- Another panellist noted it is not the quantity of initiatives that matters, but collaboration is key to ensure efforts are not duplicated and that the initiatives complement each other. Companies must, however, still exercise due diligence as an individual company and know their specific risks and leverage.

3.2 Challenges for the ICT Sector Associated With Mass Surveillance Revelations

- Recent revelations and allegations of mass surveillance have consumed the debate around privacy and freedom of expression in the ICT sector. One panellist commented that at the recent Freedom Online conference in Tunisia, the agenda "had to be ripped up and started again" once the revelations came to light.

- Mass surveillance operations by governments worldwide implicate companies which own the infrastructure and store the data governments seek to access. Some ICT companies do publish 'transparency reports' which give information on the number of times governments worldwide have requested user information or content to be taken down, and publish the percentage of requests a company has complied with. However, under the US Foreign Intelligence Surveillance Act, US government orders to companies are secret and companies are unable to even acknowledge the existence of such orders and therefore they do not feature in transparency reports. Internet companies, telecommunications companies and undersea cable operators, through which 90% of internet traffic flows, appear to have been given orders to allow law enforcement to intercept communications on a massive scale. One business representative from the audience also spoke of a government that set up a fake base station to capture all traffic, illustrating how widespread this practice of mass surveillance appears to have become.

- Given these developments, what should companies be doing about it? Another participant agreed that even though this issue is particularly difficult, “a dilemma is not an excuse for inaction” adding that consumer pressure would help ensure that companies respond. But one participant questioned the power of the consumer in this sector as compared to apparel, for example. They commented that some services offered in the ICT sector are different from other sectors in that the users are not customers. For example, it is advertisers that provide revenue for Facebook, not users. This limits the possibility for effective user pressure.

- One participant pointed to a report by the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, on surveillance, released a few months before the revelations came to light, which says,

> “*Costs and logistical hurdles to conduct surveillance on a mass scale continue to decline rapidly, as technologies allowing for broad interception, monitoring and analysis of communications proliferate. Today, some States have the capability to track and record Internet and telephone communications on a national scale. By placing taps on the fibre- optic cables, through which the majority of digital communication information flows, and applying word, voice and speech recognition, States can achieve almost complete control of tele- and online communications. Such systems were reportedly adopted, for example, by the Egyptian and Libyan Governments in the lead-up to the Arab Spring”*[19]

- The participant framed the dilemma: targeted surveillance is only allowed in limited, necessary and proportionate circumstances so human rights norms suggest this practice of mass surveillance is not allowed, yet orders that result in mass surveillance are served by governments that have signed these human rights treaties. This puts companies in a difficult position. The participant asked, “To what level are companies pushing back, that’s what I’d be asking companies to do, even though you may be gagged, what actions can you take?”

- One panellist said the recent revelations have “blown apart the obsession with secrecy” and that “companies should always be pushing back against secrecy of demands that either fly close to the line or break the line of human rights standards.”

- Participants agreed that companies were expected to, in light of the revelations, push for further transparency regarding the requests made to them by governments that may impact negatively on respect for privacy and other rights online.

3.3 The Importance of Transparency Concerning Government Requests

- It was agreed that one action companies can take is to be transparent to the fullest extent possible about what they are being asked to do by governments. One panellist said that transparency improves confidence in governments while secrecy “undermines the ‘western’ case for privacy and freedom of expression around the world, making it easier for other governments to ignore laudable freedom of expression initiatives.”

- As the recent revelations focus on secret orders, so secret that companies could not even acknowledge the existence of them, the question was asked, is it possible to be

[19] http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

transparent? One panellist said that while transparency is important, companies can often only go so far, that it is possible to be transparent about laws and how they work but further action is out of a company's knowledge or operational control. The panellist detailed a particular company's efforts to publicly explain how SORM (System for Operative Investigative Activities) works and the risks it presents for companies in respecting human rights. SORM is a system for intercepting telephone and Internet communications, developed by the Soviet Union and still employed in Russia and some ex-Soviet states. It allows law enforcement to place a 'black box' directly on the network to gather information after seeking a warrant from the court. Having direct access to a network removes the need to serve a warrant on the network operator to intercept and provide information to law enforcement. The panellist said that SORM cuts out the operator from being part of the interception process and interception is done without the company's knowledge. Therefore, companies do not know what kinds of requests are being made to the courts, making it impossible to push back on requests. The panellists said that companies should be able to reach out to the general prosecutor granting the warrants to law enforcement.

- This approach was contested by another participant, highlighting the wide range of opinions on how companies are expected to respond not just to individual requests, but to structuring and operating infrastructure. The participant argued that it is not appropriate for any company to say they do not have responsibility when they have provided full access to their network, which allows for indiscriminate mass surveillance. They argued that by going far enough down the company to the engineers, a company can identify the kinds of requests law enforcement are carrying out through SORM as any change in the flow of information through a network can be identified; if it could not, the company could not function. The precision of the company's control in these circumstances was contested.

- It was generally agreed that it is extremely important that companies in the ICT sector leverage the opportunity provided by the recent revelations to push governments to be allowed to be transparent to the fullest extent possible and that companies are expected to adhere to human rights standards, even when that means going beyond just abiding by the law.

3.4 Challenges for NCPs in the ICT Sector

- NCPs are widely known as the "implementation arm" of the OECD Guidelines.[20] The first panel laid out some of the dilemmas facing companies in the ICT sector and it was acknowledged that NCPs will increasingly have to grapple with these issues in their work; the speed of industry growth and global span can make it difficult to keep track of developments.

- The ICT sector is a new field for NCPs, which historically have dealt primarily with environmental and labour issues. There is no body of similar cases among other NCPs dealing with ICT related issues, as exists in other sectors such as extractives. The technical aspects may be unfamiliar to NCPs, yet it is expected that NCPs will receive a significant number of cases relating to the ICT sector in the coming years given it is one of the fastest growing sectors.

[20] OECD (2012) Annual Report on the OECD Guidelines for Multinational Enterprises 2012: Mediation and Consensus Building. OECD Publishing, Paris, p 8.

- It was also noted that the ICT sector is one of the few sectors where SMEs can have a significant impact on human rights, given the potentially wide reach of technology without it being necessary to have a physical presence on the ground in the country of operation. NCPs can therefore expect to be faced with cases involving companies who are quite unfamiliar with the OECD Guidelines and the international human rights framework underlying the Guidelines.

3.5 Addressing the First ICT Complaint to an NCP Relating to Surveillance Technology

- Panelists included a civil society representative who had filed a complaint with the UK and German NCPs regarding two companies selling surveillance technology to the government of Bahrain. The complaint alleges the government of Bahrain then used the technology to access the communications of pro-democracy activists and dissidents, which in some cases led to their exposure, arrest and torture. The complaint cites the sale of the products as a violation of the OECD Guidelines. The complaint brought to the UK NCP will go to the mediation process. This is the first complaint of its kind brought to an NCP.

- The panellist gave some background on bringing the complaint and attempts to engage the companies in presenting their concerns about human rights violations linked to the sale of these products to the government of Bahrain. The organisation concluded that the most appropriate way to engage the companies was in public and it was thought the OECD Guidelines were a “good fit”. Commenting on the overall experience of engaging with the process and submitting the complaint to the NCPs, the participant praised the NCPs involved, saying he “couldn’t speak highly enough” of them.

3.6 Shaping Robust NCP Responses in the ICT Sector

- **Using existing guidelines and initiatives:** One panellist spoke of an emerging “normative framework” to help NCPs clarify their expectations of companies in the ICT sector when it comes to respecting the OECD Guidelines. The European Commission Guides on Implementing the UN Guiding Principles on Business and Human Rights for both the ICT sector and Employment and Recruitment Agencies sector was referenced, as well as the GNI guidelines.

- **Understanding the power balance in the mediation process**: One panellist highlighted the importance of not assuming that companies and workers are coming to the table with the same knowledge and resources and the need to take into account different power relations during mediation.

- **Expanding the financial consequences of final statements:** NCPs issue final statements at the conclusion of their procedures, whether there was a determination in a case or not. If a company accused of a failure to implement the OECD Guidelines did not engage with the mediation process, NCPs can still look at the complaint and make recommendations on the application of the Guidelines. Investors are increasingly looking to NCP statements to inform their investment decisions. Under the OECD Common Approaches for Officially Supported Export Credits and Environmental and Social Due Diligence that apply to Export Credit Agencies (ECAs), ECAs should consider

NCP statements before awarding export credit.[21] This has particular significance for some companies in the ICT sector because of the "dual use" nature of some technology and the need for ECA support in underwriting the sale of particular technology. A failure to engage with an NCP therefore can result in blocking or withdrawal of export finance or diplomatic assistance for companies.

- **Ensuring follow up and monitoring:** NCPs typically do have limited resources to engage in the follow up of specific instances. Participants suggested that by making final statements public, NCPs will be building up a body of widely available evidence and decisions on addressing issues in the ICT sector that can be followed up by other interested stakeholders, such as civil society.

- **Knowledge sharing among NCPs:** Participants pointed out that NCPs can consult with each other and that horizontal peer learning processes among NCPs provide a more detailed forum for sharing lessons learned. Joint NCP meetings also provide an opportunity to discuss approaches to new issues, such as those in the ICT sector, and the OECD Secretariat can play a supporting role in developing further guidance for NCPs.

3.7 Possible Remedies

- In the case of manufacturing, one panellist noted that NCPs and the OECD Guidelines are a unique mechanism that can address gaps, but are not a substitute for operational level grievance mechanisms within companies.

- One panellist noted that the major difference with the ICT sector is that remedy can be very quick. For example, an oil spill takes a long time to clean up and is extremely expensive. With the ICT sector, "a flip of a switch can change things." The participant went on to explain that some technology is updated weekly or routinely from companies' central offices, therefore all of this technology has a shelf life. If updates stop, the technology does not work, therefore abuses stop. Some products have built in 'kill-switches', which could be used to prevent further abuse.

- Another participant highlighted that when companies do decide to divest interests in companies selling surveillance technology, they should not just divest the name and profits, but take additional steps to ensure abuses do not carry on under a new company's name. Simply selling off the problem is not enough.

4. Conclusions

The sessions reflected the current debate around the challenge of surveillance, with regard to both the recent allegations of mass surveillance by governments and the roles of ICT companies, and the first complaint brought to NCPs concerning the sale of surveillance technology to governments by companies. Although the process of understanding the ICT sector in relation to the OECD Guidelines is still at early stages, the potential impact of NCPs in providing a space for complaints to be brought and ensuring access to remedy is clear.

[21] OECD Working Party on Export Credits and Credit Guarantees, Recommendation of the Council On Common Approaches For Officially Supported Export Credits And Environmental And Social Due Diligence (The "Common Approaches"), Section V, 15, http://search.oecd.org/officialdocuments/displaydocumentpdf/?cote=TAD/ECG%282012%295&doclanguage=en

A number of specific conclusions from the discussions regarding next steps should also be noted:

- There is a need to draw on existing guides and initiatives to improve NCPs' own understanding of the ICT sector and to strengthen their role in promoting the OECD Guidelines to the sector.

- Greater efforts should be dedicated to promoting in particular the importance of transparency as outlined in the OECD Guidelines.

- Companies seeking investment or export credit should be informed of the importance of engaging with NCPs and NCP final statements.

- There is significant value in promoting further sharing of knowledge and case studies amongst NCPs to build up their collective expertise on dealing with complaints related to the ICT sector.

- Explore remedies that use the speed of technological development to provide quick or instant remedy. For example, if companies ceased to supply software updates to users known to be using their products to violate human rights, the technology would not work and abuses could quickly stop.

- More attention should be given to raising awareness among SMEs in the ICT sector that may have a particular impact on human rights.

Annex I

Agenda

Multinational enterprises, human rights and Internet Freedom

Paris, 27 June 2013, 14.30-16.30

Panel One: 14.30-15.30: Cooperative efforts to promote Internet freedom

- John Kampfner, Global Network Initiative, USA/UK
- Marie Baumgarts, Tele2 (on behalf of the Global e-Sustainability Initiative)
- Christine Diamanté, Alcatel Lucent (on behalf of the "Telecommunications Industry Dialogue")

Chair: John Morrison (Executive Director, IHRB)

Panel Two: 15.30-16.30: OECD National Contact Points and interpreting the Guidelines in relation to the ICT sector – why it matters

- Laura Ceresna, Policy Advisor, CIVIDEP, Bangalore, India
- Eric King, Privacy International, UK
- Roel Nieuwenkamp, Foreign Ministry of the Government of the Netherlands

Chair: Margaret Wachenfeld (Director of Legal Affairs, IHRB)

END