Department for Business Innovation & Skills

Institute for Human Rights and Business
Shaping Policy ▪ Advancing Practice ▪ Strengthening Accountability

MEETING REPORT:
OECD National Contact Points and the ICT Sector

Friday, 10 July 2015
UK National Contact Point, Department of Business, Innovation and Skills, Conference Suite, 1 Victoria Street, London SW1H 0ET

Table of Contents

Introduction

The Organisation for Economic Co-operation and Development (OECD) Guidelines for Multinational Enterprises (the "OECD Guidelines")[1] are the most comprehensive set of government-backed recommendations on responsible business conduct. The Guidelines aim to encourage the positive contributions businesses can make to sustainable development while minimising the negative impacts of their operations and their business relationships. The 2011 revision to the OECD Guidelines includes an entirely new chapter on human rights that builds on the United Nations Guiding Principles on Business and Human Rights (UNGPs)[2] and strengthens the possibility of bringing cases for mediation to NCPs established pursuant to the OECD Guidelines.

Adhering governments make the commitment to establish a National Contact Point ("NCP"). NCPs play a unique role of providing a grievance and mediation mechanism that contribute to the resolution of issues that arise from the alleged non-observance of the OECD Guidelines by OECD-based multinationals. These are referred to in the OECD Guidelines as "specific instances". The NCPs also further the effectiveness of the OECD Guidelines by undertaking promotional activities and handling enquiries about the Guidelines.

The 2011 revision, as part of the General Policies section, encourages companies to, *"support, as appropriate to their circumstances, cooperative efforts in the appropriate fora to promote Internet Freedom through respect of freedom of expression, assembly and association online*."[3] In addition, the section on consumer interests states that companies should, *"respect consumer privacy and take reasonable measures to ensure the security of personal data that they collect, store, process or disseminate."*[4]

On 10 July 2015, the Institute for Human Rights and Business (IHRB) together with the UK NCP based in the Department for Business, Innovation & Skills (BIS) brought together a range of OECD National Contact Points (NCPs), businesses within the ICT sector, and trade union and civil society organisations focused on NCP "specific instances" for a fourth meeting of stakeholders since the establishment of the updated OECD Guidelines for Multinational Enterprises (the OECD Guidelines) in 2011. The event was facilitated by IHRB and discussed the OECD's work in the ICT sector, in particular building on the first ICT-related complaints to the UK NCP in 2013. This is the first time this annual workshop has focused on the ICT sector.

[1] http://www.oecd.org/daf/inv/mne/48004323.pdf
[2] http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf
[3] http://www.oecd.org/daf/inv/mne/48004323.pdf, Section II General Policies, para B.1, p20
[4] Ibid, Section VIII Consumer Interests, para 6, p51

Opening Comments

Mr. Jeremy Carver, a member of the Steering Board for the UK NCP, opened the event with a few words on the challenges presented by the ICT sector, highlighting in particular the speed of change in the ICT sector. He noted with interest the updating of the OECD Guidelines in 2011 to include the relationship between technology and human rights.

Panel I: An Overview of Key Developments on Human Rights and the ICT Sector Relevant to the Application of the OECD Guidelines on MNEs

This session covered key developments relevant for companies and NCPs to consider in thinking about the responsibility of MNE in the ICT sector, in particular latest domestic and international cases, reports and standard setting.

Professor. Roel Nieuwenkamp, Chair of the OECD Working Party on Responsible Business Conduct, opened the first panel with an overview of the OECD's scope of work in the ICT sector, covering the life cycle of a mobile phone, from the minerals used to produce mobile phones to the e-waste produced when phones are disposed. This life cycle touches on all chapters of the OECD Guidelines, from supply chain, to labour, to environment. He noted that as reporting on conflict minerals will soon be mandatory for companies (through Dodd Frank and EU regulations), this issue is high on the OECD's agenda. As China has most of the smelters, outreach here is important.

He further emphasised that the work of the OECD does not just focus on a responsible *supply chain*, but also a responsible *value chain*. The recent complaint brought to the UK NCP regarding the technology company Gamma and the sale of surveillance technology to Bahrain reflects the shift from supply chain to wider value chain.[5] In this case, the complaint was not about what the company bought (which

***The OECD Guidelines** state that:*

Enterprises should:

• Carry out **risk-based due diligence**, (...), to identify, prevent and mitigate actual and potential adverse impacts (...), and account for how these impacts are addressed.

• **Avoid causing or contributing to adverse impacts** on matters covered by the Guidelines, through their own activities, and address such impacts when they occur.

• **Seek to prevent or mitigate an adverse impact** where they have not contributed to that impact, when the impact is nevertheless **directly linked to their operations, products or services by a business relationship.**

[5] https://www.gov.uk/government/publications/uk-ncp-final-statement-privacy-international-and-gamma-international-uk-ltd

refers to the supply chain) but rather what it sold (which refers to the value chain).

Prof. Nieuwenkamp explained that the OECD prefers to use the term 'responsible business conduct' throughout the organisation, as it is felt the term corporate social responsibility (CSR) has a voluntary or philanthropic connotation. Instead, the OECD Guidelines have a binding grievance mechanism and promotional mechanism through the NCPs, which is married to the International Labour Organisation (ILO)'s international labour standards and the UNGPs.

Prof. Nieuwenkamp then outlined the common understanding of what is meant by due diligence, with a five step approach to due diligence in the supply chain:

1. Adopt strong management systems
2. Identify, assess and prioritise risks
3. Manage risks
4. Verify due diligence
5. Communicate and report on due diligence

The advice to companies subject to an OECD complaint is to come to the table, as it is always good to engage with stakeholders and the NCP. While the OECD Guidelines are non-binding there can be consequences for companies regarding:

- **Reputation**: For example, the draft statement by the Chilean NCP over Starbucks led to a resolution whereby the parties eventually reached an agreement and signed the first collective bargaining agreement of Starbucks Chile SA and its union.[6]
- **Financial:** For example, the stock market moved following a statement from the UK NCP regarding the security company G4S[7]. Institutional investors could divest, or at the least begin to ask questions. The statement on mining company Vedanta led to divestments from prominent institutional investors. [8]
- **Government support:** OECD governments should take into account NCP statements. The 'OECD Common Approaches for Export Credit agencies' state that Export Credit Agencies should promote the OECD Guidelines and that they should take into account NCP statements. For example, at the start of 2014 the mining company China Gold refused to engage with the Canadian NCP or respond to inquiries. Due to this, the Government of Canada's CSR strategy launched in November 2014 included new measures that any cases of non-participation in the NCP process will be taken into consideration in any applications by China Gold for advocacy support or export credit.[9]

[6] http://www.tuacoecdmneguidelines.org/CaseDescription.asp?id=179
[7] http://oecdwatch.org/cases/Case_340
[8] http://www.oecd.org/investment/mne/43884129.pdf
[9] http://www.international.gc.ca/trade-agreements-accords-commerciaux/ncp-pcn/statement-gyama-valley.aspx?lang=eng

Mr. Alan Krill, Foreign Affairs Officer, Internet Freedom, Business, and Human Rights Team, Bureau of Democracy, Human Rights and Labour, U.S. Department of State, then presented the perspective of the US NCP, which has not yet had any specific instances involving the ICT sector. Mr. Krill referenced the promotional function of the NCP with regards to human rights due diligence. The June 2015 G7 leaders vision statement[10] dedicated a whole section to human rights due diligence and committed to strengthening mechanisms for providing access to remedies including the NCPs. The G7 will encourage the OECD to promote peer reviews and peer learning on the functioning and performance of NCPs.

Mr. Krill noted that the ICT sector can be a complicated sector to apply the OECD Guidelines, which do reference internet freedom. There is also a much broader conversation going on about ICTs and human rights outside of the NCP context. He referenced three developments in the ICT Sector that have had an impact: **multi-stakeholder collaboration; transparency reporting; national action plans.**

1. Multi-stakeholder Collaboration

The Freedom Online Coalition[11], a coalition of 27 governments (at the time of the meeting) committed to advancing freedom online, including through the 2014 Tallinn Agenda[12], have recently extended the mandate of a Privacy and Transparency Working Group, currently with members from government, business and civil society, to help put the principles outlined in the Tallinn Agenda into practice. The Coalition has released statements on, among other topics, spyware[13] and Internet restrictions on social media platforms[14] that can help contextualise issues for the NCPs.

There have also been efforts to launch a multi-stakeholder discussion on the role of ICT companies in removing alleged "extremist" content and new anti-terror laws. Mr. Krill referenced the launch of a policy dialogue by the Global Network Initiative and the Telecommunications Industry Dialogue on "Extremist Content and the ICT Sector".[15]

[10] https://www.whitehouse.gov/the-press-office/2015/06/08/g-7-leaders-declaration
[11] www.freedomonlinecoalition.com
[12] https://www.freedomonlinecoalition.com/wp-content/uploads/2014/04/FOC-recommendations-consensus.pdf
[13] Freedom Online Coalition, September 2014, Joint Statement on on the Use and Export of Surveillance Technology https://www.freedomonlinecoalition.com/wp-content/uploads/2014/10/2-FOC-Joint-Statement-on-the-USe-and-Export-of-Surveillance-Technology-October-2014.pdf
[14] Freedom Online Coalition, August 2014, Joint Statement on Restrictions on Access to Social Media https://www.freedomonlinecoalition.com/wp-content/uploads/2014/08/FOC-statement-on-restrictions-on-access-to-social-media.pdf
[15] https://globalnetworkinitiative.org/sites/default/files/Extremist%20Content%20and%20the%20ICT%20Sector.pdf

2. Transparency Reporting

A growing number of companies in the ICT sector are publishing annual or bi-annual reports showing how they comply with requests received from law enforcement agencies worldwide to hand over user data or take down content. These are known as 'transparency reports'. Mr. Krill referenced the growth of both companies and governments releasing transparency reports. He also noted that the USA Freedom Act has a provision for transparency reporting for both the government and companies.[16]

3. National Action Plans

The USA is committed at the highest level to drafting and publishing the National Action Plan (NAP) on Responsible Business Conduct.[17] He referred to the guidance on *Assessing Cybersecurity Export Risks*, published by the UK Government and industry association techUK, as a good model of a commitment identified in the UK National Action Plan that was then turned into concrete guidance.[18] On that subject, the USA is soliciting comments on proposed rules implementing recent ICT-related controls agreed to by the multilateral Wassenaar Arrangement.[19]

Mr. John Davies, Director Strategy and Government Relations at BAE Systems Applied Intelligence then presented the business perspective. He said of all the products and services the company sells, it is those that facilitate surveillance that have the most scope for being misused and which therefore take the most internal considerations before sales are approved. He noted that the company was large enough to have a good relationship with UK government, which helped with due diligence on foreign customers – something smaller companies may struggle with.

Mr Davies outlined the drivers that any UK business in this area had to cope with:

1) Winning new work by offering capabilities that meet a real need;
2) Doing a good job for that customer – meeting their need reliably and effectively;

---

[16] https://www.congress.gov/bill/113th-congress/house-bill/3361/text See TITLE VI—FISA TRANSPARENCY AND REPORTING REQUIREMENTS, Section 602 and 603.

[17] "In the field of business and human rights, a NAP is defined as an "evolving policy strategy developed by a State to protect against adverse human rights impacts by business enterprises in conformity with the UN Guiding Principles on Business and Human Rights (UNGPs)." UN Working Group on Business and Human Rights, Guidance on National Action Plans on Business and Human Rights, December 2014. http://www.ohchr.org/Documents/Issues/Business/UNWG_%20NAPGuidance.pdf

[18] https://www.techuk.org/images/CGP_Docs/Assessing_Cyber_Security_Export_Risks_website_FINAL_3.pdf

[19] The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies is a multilateral export control regime (MECR) with 41 participating states. It was established to contribute to regional and international security and stability by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies. https://www.federalregister.gov/articles/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items#addresses

3) Working with the UK export authorities, both to get help (and increase 'good' security exports), and to get approval for export licences;
4) Not over-selling. Designing the capability to do the job well, but not overdoing it – both from a risk-mitigation stance, and from a good-engineering stance.

He outlined some of the possible approaches considered by the due diligence process around a new customer:

1) Not selling at all, where the delivery would just be too risky. This does not help the customer at all.
2) Selling a constrained system to reduce the risk of misuse, if that is possible;
3) Limiting the after-sale support period to allow disengagement if serious misuse were to occur.

He said that none of these options were very attractive, particularly when facing competition from other companies and countries, so selling this type of capability only to customers where the company (and UK government) has a strong track-record and customer relationship, and even an office presence, was their preferred approach.

Mr Davies raised some questions around how any company disengagement could practically occur, if the worst happened. Would the company withdraw from a contract and customer forever? For a fixed time, or until significant changes had occurred? It seemed very unclear how that would work in practice.

Mr Davies concluded that sales in this area will never be zero risk. Following the guidance and doing the due diligence does help greatly, but the eventual business decisions on helping a customer or not, or continuing to support the customer or not, could still be very difficult.

Mr. John Morrison, moderating, added that companies must also explore how transparent they can be, especially if there is always a risk. But this is of course a challenge where national security is involved.

Ms. Gabrielle Guillemin, Senior Legal Officer at ARTICLE 19[20], then gave a presentation on developments at the European and international level, and why protection for human rights defenders in the age of digital surveillance is so important.

Firstly, Ms. Guillemin praised the pioneering work of the OECD Guidelines and the work done by the organisation since the 1960s, including setting the groundwork for the European data protection directive, which is so important in the digital age.

Ms. Guillemin highlighted recent work at the United Nations, including the appointment of a Special Rapporteur on Privacy, Mr. Joseph Cannataci. The UN

[20] http://www.article19.org

Resolution on Right to Privacy in the Digital Age[21], which proposed creating the Special Rapporteur for Privacy, makes clear that the Special Rapporteur will be working closely with companies.

Ms. Guillemin also highlighted the recent thematic report by the Special Rapporteur for Freedom of Expression, Mr. David Kaye, on the importance of encryption and anonymity for the enjoyment of freedom of expression.[22] In addition, a good resource for NCPs is the Ranking Digital Rights project,[23] which is about to publish its first Corporate Accountability Index, which ranks 16 of the largest internet and telecommunications companies according to indicators focused on corporate disclosure of policies and practices that affect users' freedom of expression and privacy.

Ms. Guillemin went on to explain that human rights protections are not just theoretical, they have very real impacts. She cited the recent example of the UK intelligence agency GCHQ, which was found to have intercepted the communications of staff at Amnesty International and the Legal Resource Centre in South Africa, which works on issues of social justice.[24] She described the impact it has had on their ability to communicate with members and representatives and that the organisations have not been given an explanation as to why this has happened.

ARTICLE 19 works with organisations based in Pakistan, Azerbaijan and other countries where journalists and human rights defenders may be branded terrorists under the law, eg. Ethiopia. Anti-terror laws are typically being used to target activists and dissenters, which in turn may result in the interception of communications with international NGOs through the use of spyware being discussed today. This is an on-going difficulty as there is a conflict between domestic laws that may be criminalising expression, and the international law that protects it.

Finally, Ms Guillemin highlighted some of the limits of existing mechanisms to challenge cyber exports. In particular, information about the sale of surveillance technology is usually treated as confidential information. In the absence of a requirement to obtain a license to export such products, information about these transactions is therefore hard to trace. This lack of identifiable chain of sale and export tends to significantly undermine the case of civil society organisation seeking to protect or obtain a remedy for partners living in Bahrain and other countries and who are subject to surveillance.

There was a robust discussion following the first panel.

- One participant commented that the space for civil society to operate is shrinking, due to laws essentially criminalising their operations, but that the

[21] http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx
[22] http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx
[23] https://rankingdigitalrights.org/
[24] http://www.theguardian.com/uk-news/2015/jul/01/gchq-spied-amnesty-international-tribunal-email

safety of human rights defenders is the priority of some governments worldwide.

- One participant asked whether the OECD would consider producing guidance for the ICT sector and raised the issue of short term and long term impacts on human rights. The example given was that the surveillance industry is a thriving and growing market, particularly in difficult markets. If a company decides to divest that part of their company and stop selling surveillance technology in those markets, in the short term this is positive, but another company with perhaps less of an eye on human rights and due diligence might step into that market, which in the long term would be bad for human rights.
- The response to this comment was that the OECD cannot produce guidance for every sector, unless they had the support and request of all 46 members, so instead it presents a common understanding of expectations of companies through the OECD Guidelines and the five due diligence steps highlighted above.
- Another participant asked whether the OECD NCP mechanism was in fact fit for purpose in the age of mass surveillance. This was because any mediation requires transparency, but the issue of mass surveillance is shrouded in secrecy. One participant responded that confidentiality is a core business interest and this is an essential area of protection in the NCP process. The process will develop because it is an international process recognising only one way forward, and that is consensus. Another questioned whether it is possible to identify a "specific" instance where there is an on-going government programme of surveillance.

Panel II: Lessons learned on the application of the OECD Guidelines in the ICT Sector

This session discussed recent cases from the ICT sector brought to OECD NCPs and any lessons learned. The session also discussed the difficulties in bringing a complaint and responding, and key issues that NCPs should be aware of.

Ms. Liz Napier and Mr. Danish Chopra of the UK NCP presented the work of the UK NCP, giving the example of a 2013 complaint regarding six telecommunications companies.[25] The OECD Guidelines are clear that companies should address adverse impacts to human rights that are either caused or contributed to by the enterprise, or are directly linked to their operations, products or services by a business relationship. In this case, the business relationship was with a government agency.

The UK NCP took on an extra member of staff to help provide support on these complaints, and made a decision in July 2014 to reject the complaint. The main reason for this was that the NCPs felt the evidence presented was not substantiated.

[25] https://www.gov.uk/government/publications/uk-ncp-initial-assessment-complaint-by-an-ngo-against-6-uk-based-telecommunication-companies

The evidence submitted was based on whistleblower evidence, but that whistleblower was more concerned about the government role than the company role and so on this basis the complaint was rejected.

Ms. Napier and Mr. Chopra questioned whether the NCP process was the best vehicle to have used in this case. The NGO bringing the complaint was not representing an individual, but all users of the six telecommunications companies and it was not clear who had been harmed. NCPs are not experts, they could buy in expertise but are concerned about the differing opinions of experts. It may be that even though a judgement is needed, NCPs are unable to make one. Mr. Chopra said that companies needed to be more open to the complaints process, but ultimately this is a voluntary process. On the other side of the coin there is the issue of security. There is an argument that there is not enough security and if ICT companies give more information to governments, the government could protect human rights more. This puts the NCPs in the position of being an avenue to express political grievances, which is not the reason they exist.

Mr. Malte Hauschild, the German NCP, then gave a perspective of his work. The German NCP has existed since 2001 and has received 33 cases. Eleven of these cases were received since the OECD Guidelines were revised in 2011. These cases had a strong focus on labour, mainly covering trade unions. Usually, the NCP will spend 3 months assessing the case and 9 months to deliver a judgement.

Mr. Hauschild gave the example of a case brought by 5 NGOs to both the German NCP and the UK NCP, where a surveillance company had provided maintenance capabilities in 2009 and onwards, to the government of Bahrain during the revolution. This case was only partially accepted in relation to the allegation that the due diligence provisions had not been sufficiently fulfilled. The NCP did not accept that the company had violated the Guidelines and considered that the evidence provided was insufficient. He pointed out the software at issue was lawfully allowed in Europe (and in fact required), therefore it was important to show the specific connection to the human rights abuse. The complainants then withdrew from the process as they did not agree with the partial acceptance, so the case was closed.[26] The NCP regretted that behaviour. The case had nevertheless further implications: The issues at stake were also discussed in the Wassenaar Agreement. In view of the seriousness of the issues an expanded German caveat was introduced with the need of an export licence for exports of surveillance technology.

Ms. Caroline Wilson Palow, General Counsel at Privacy International, then provided the NGO perspective on bringing a complaint to an NCP. While not involved with the complaint presented by the UK NCPs regarding six telecommunication companies, Ms. Wilson Palow presented the same example as detailed by Mr. Hauschild, detailing the sale of surveillance technology to Bahrain, which was simultaneously submitted to the German and UK NCPs. While the German NCP partially accepted

[26] http://oecdwatch.org/cases/Case_287

the complaint, the UK NCP found that there had been a violation of the OECD Guidelines.

Ms. Wilson Palow said that while recognising the NCP complaint process is an imperfect grievance mechanism, it is one of the few available, and noted that in the USA, there is immunity from prosecution for companies co-operating with the US on surveillance issues.

Ms. Wilson Palow said that one of the difficulties in bringing complaints regarding surveillance is that lot of the information is based on leaked information, which is hard to verify. In addition, the process did not compel the company to disclose that they did sell the technology in question. Providing evidence was a big challenge; the organisation tried to come up with the best evidence possible, including trying to prove the technology was sold to Bahrain by providing timelines and evidence that the technology in question was present on the devices of activists. Ms. Wilson Palow suggested that NCPs do not have to be as rigorous with evidence as in a court of law, if they are only providing advisory opinions, pointing out the UK's Investigatory Powers Tribunal (IPT)[27] will hear cases about hypotheticals.

Ms. Wilson Palow said that the companies are seen as one of the first lines of defence in this area and responsible people in the company are needed who would engage with the mediation. As Internet companies are pushing back on US government surveillance, this is something that Privacy International would like to see in other areas.

Ms. Kristen Genovese, Senior Researcher at OECD Watch[28], presented some lessons learned from 15 years of NCP cases globally from their recent report *Remedy Remains Rare*.[29] Some highlights include:

- The most NCP complaints were submitted in 2013, a total of 44.
- Of all the complaints submitted over the years, the highest number are regarding human rights issues (186)
- The mining industry received the most complaints (56), followed by:
    - Oil and Gas (33)
    - Financial Institutions (29)
    - Agriculture Companies (23) and
    - Garment Companies (13)
- Since the revised OECD Guidelines in 2011, there have been 15 ICT related complaints. Out of these 15 complaints, 12 were rejected.
- 10 of these complaints were submitted to the UK NCP.

[27] The IPT is a court which investigates and determines complaints of unlawful use of covert techniques by public authorities infringing the right to privacy and claims against intelligence or law enforcement agency conduct which breaches a wider range of human rights. http://www.ipt-uk.com/default.aspx

[28] www.oecdwatch.org

[29] http://oecdwatch.org/publications-en/Publication_4201

- The first case against a telecommunications company was submitted to the Mexican NCP in 2012
- From 2012-2015, 52% of all complaints were rejected. The most frequent reason was “insufficient substantiation”

Ms. Genovese presented a set of recommendations for NCPs including:

1. Determinations of non-compliance with the Guidelines. If the case is not amenable to mediation or if mediation fails, NCPs should make determinations of non-compliance with the Guidelines based on independent investigations.

2. Incentives and disincentives for non-compliance. Member and adhering governments should ensure that findings of non-compliance result in material consequences, such as the withdrawal of trade services.

3. Admissibility criteria. NCPs should refrain from adding admissibility criteria beyond what is stated in the Procedural Guidance and should not interpret those criteria to require excessively high standards of proof at the initial assessment stage.

These recommendations can be achieved through:

- The OECD Investment Committee should require NCPs to undergo a peer review at least once every five years. Until a mandatory system is instituted, NCPs should volunteer for peer review, beginning with the G7 NCPs.
- Ultimately, OECD Watch calls on the OECD Investment Committee to initiate a process to revise the Procedural Guidance with the objective of strengthening the NCP structure and functioning.

There followed a discussion of thresholds of evidence and the purpose of the NCP system.

- One participant questioned the notion that there had to be an identifiable victim in the cases, when NCPs are only judging on whether there had been a violation of the OECD Guidelines.

- Another participant disagreed that evidentiary standards are too high, but more than a newspaper article is needed.

- One participant noted there is an OECD complaints mechanism under the OECD Guidelines for civil society and trade union against NCP’s that are allegedly not fulfilling their procedural responsibilities under the Guidelines. It has never been used yet, but it is a possibility for addressing issues, like ‘burden of proof has been set too high’.

- One participant stressed that the appropriate interpretation of ‘material and substantiated’ for NCP’s to accept complaints should be that a complaint is plausible. Full proof beyond reasonable doubt is not necessary.

- One participant observed that as no liability is being decided upon, the evidentiary standard should be something less than in a civil case which is what the NCPs seem to be requiring.

- One participant pointed out the link between the two companies selling the surveillance technology to Bahrain, one in the UK and one in Germany. When combined, there is more potential for abuse when there are two products, so how did the UK and German NCP coordinate?

- One participant said that the OECD Guidelines are not a legal framework and when the Guidelines were established in 1976, the idea was to have a mechanism that does not feed into court system, which would be onerous and expensive. There was a strong resistance from some participants on making the process more legalistic.

- One participant noted that one of the main strengths of the NCP is starting a dialogue, as NGOs are often unable to reach out to companies and are ignored. It depends on the measure of success – is it cases resolved or company-NGO dialogues started? Or is it about remedies that communities are satisfied with rather than just what the company is prepared to provide? One participant expressed concern that there seemed to be few changes on the ground as a result of NCP decisions, highlighting that comparative research with the development finance institutions showed that their mediation processes resulted in more changes on the ground.

- One participant asked what weight is given to a company's human rights due diligence policy rather than evidence of complainants. Another participant responded that the process is to look at what policies a company has in place, how they have delivered on the policy, what standards they have referred to. It also depends on what the complaint is about -- sometimes it is about the lack of due diligence, or that due diligence has been done but there has been a violation.

Panel III: Guidance for NCPs, Businesses and Civil Society on the Responsibility to Respect Human Rights in the ICT Sector

The purpose of this session was to introduce forums and resources that could assist the OECD NCPs in finding out more information about the ICT sector.

Ms. Judith Lichtenberg, Executive Director of the Global Network Initiative (GNI)[30], introduced the GNI and presented some recent examples of the GNI's work. The GNI is a multi-stakeholder group of companies, civil society organisations (including

[30] www.globalnetworkinitiative.org

human rights and press freedom groups), investors and academics, working to protect and advance freedom of expression and privacy in ICTs.

The GNI provides:

1. A principled approach to guide company responses to government requests impacting user rights
2. Accountability through independent assessment
3. A platform for collective policy engagement
4. Unique opportunities for shared learning

Outputs consist of:

- Core documents of GNI Principles, Implementation Guidelines, Accountability, Policy & Learning Framework
- Annual reports
- Public Assessment reports
- Transparency reports from member companies
- Publications (submissions, letters, statements, research reports) Videos and Commentary

Ms. Lichtenberg then presented some examples of how the GNI works in practice.

Microsoft in Russia

In 2009, GNI member Human Rights First was made aware by sources in Russia that the offices of activists, human rights defenders and independent media were being raided and staff arrested for using pirated Microsoft software. The cases provided clear evidence of a pattern of selective enforcement of antipiracy laws by Russian authorities as a way to silence dissent and suppress free speech. Working with Human Rights First through the GNI network, Microsoft (another GNI member) created a new unilateral software license for civil society organisations to prevent this happening in the future. The partnership between Microsoft and Human Rights First enabled the swift identification of selective enforcement, timely intervention by Microsoft, and prompt resolution.[31]

India

India's IT Act was challenged in 2015, due to a controversial provision that was seen as retricting freedom of expression. In March, the Supreme Court of India struck down as unconstitutional Section 66a of the IT Act, which provided the power to arrest individuals for posting allegedly "offensive" content, and which had been used to arrest individuals for posting content on Facebook and other social networks. This ruling referred to an economic report commissioned by the GNI on India's IT Act[32],

[31] http://www.humanrightsfirst.org/wp-content/uploads/pdf/HRF-Msoft-Russia-report.pdf
[32] https://www.globalnetworkinitiative.org/news/gni-welcomes-landmark-freedom-expression-ruling-supreme-court-india

which concluded that changes to IT Act could add $41 billion to India's GDP by 2015.[33] It collaborated with the Internet & Mobile Association of India on an interactive slideshow to explain about India's IT law for its members.[34]

Response to the Snowden Revelations

Following the revelations in 2013 of government surveillance practices and the involvement of ICT companies, the GNI has pressed USA and other governments to be more transparent and fostered collaboration between ICT companies and civil society. GNI is seeking reforms to end of bulk collections of communications and recent reform of the US Freedom Act to end bulk collection of domestic phones records by the NSA and replaced with a program requiring specific requests to be made to telecoms companies show this is possible.[35] The GNI is also seeking commitment from the Freedom Online Coalition governments to be more transparent.

Mr. John Guelke of the University of Warwick, presented the EU SURVEILLE project which could provide assistance or be a useful source of information for NCPs.

EU SURVEILLE[36], which wrapped up in July 2015, is a free and confidential advisory service offered to technology developers and end users. It advised researchers, private companies and end users on ethical issues, legal limitations and efficiency. For example, one focus was on error and discrimination with regards to data mining, which could point suspicion in the wrong direction and result in false accusations.

The project process worked through several scenarios regarding the use of surveillance technology, devised in consultation with police and urban security experts in real cases of:

- Organized crime: drugs importation and firearms
- Counter-terrorism: NSA-type surveillance
- Urban security: regular crime, public order, smart city surveillance

The project also ran several workshops and consultations with end users, developers and civil society, which culminated in the creation of a survey of surveillance technology, presented in a colour coded and number-rated matrix. The matrix covered technology used for counter-terrorism, serious crime and local authority surveillance, assessing various scenarios and giving them a rating for usability and fundamental rights intrusion.[37]

---

[33] https://globalnetworkinitiative.org/content/closing-gap-indian-online-intermediaries-and-liability-system-not-yet-fit-purpose

[34] https://globalnetworkinitiative.org/india

[35] https://firstlook.org/theintercept/2015/06/02/one-small-step-toward-post-snowden-surveillance-reform-one-giant-step-congress/

[36] http://surveille.eui.eu/

[37] http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/surveille_d2-6_matrix_1_4/surveille_d2-6_matrix_1_4en.pdf and

Ms. Lucy Purdon, ICT Project Manager at IHRB presented the guide on *Assessing Cybersecurity Export Risks*[38], published in November 2014 by the UK government and industry association techUK. IHRB facilitated industry consultation and contributed to the drafting process.

This guidance was a planned action in the UK's National Action Plan on Business and Human Rights, which stated,

"In line with the UK Cyber Exports Strategy, develop guidance to address the risks posed by exports of information and communications technology that are not subject to export control but which might have impacts on human rights including freedom of expression on line."[39]

The guide focused on identifying and assessing risks as outlined in the UNGPs, and drew on IHRB's experience drafting the European Commission ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights.

IHRB ran several consultations with techUK company members and consulted with the International Cyber Policy Unit at the UK Foreign and Commonwealth Office.
The group mapped human rights risks in technology exports, such has those associated with capabilities such as:

- Surveillance and reconnaissance
- Analytics and big data
- Social media analysis
- Forensics
- Information operations
- Security management
- Identity and authentication
- Transaction protection and
- Trusted platforms

NCPs trying to figure out the capabilities of different products might find it useful to draw on the analysis in this guidance. Some of the risks to human rights identified included freedom of expression, freedom of association, privacy, right not to be discriminated against, right not to be arbitrarily arrested or detained, right to a fair trial, freedom from torture and the right to life.

---

http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/surveille_d2-6_matrix_8_17/surveille_d2-6_matrix_8_17en.pdf

[38] http://www.ihrb.org/publications/reports/human-rights-guidance-for-cyber-security-companies.html

[39] Good Business: Implementing the UN Guiding Principles on Business and Human Rights, HM Government, September 2013.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/236901/BHR_Action_Plan_-_final_online_version_1_.pdf

The guidance goes through the initial stages of human rights due diligence, and recommends that the risk assessment should be on-going: starting at the point of design and development, pre-sale when bidding for contracts, point of sale, and at the post-sale phase.

During the pre-sale stage, the guide recommends the human rights risk assessment process follows assessment of the 5Ps;

- Capabilities of the **Product**
- The **Place** its being exported to
- The impacts on **People**
- Assessment of the **Purchaser** and intended use
- **Partners** and sales agents.

The consultations raised many interesting but difficult questions, such as what happens when home governments encourage companies to export to places with poor human rights records, because they are allies?

Regarding due diligence on purchaser and partners ("Know Your Customer"), the companies contributed useful checklist questions and warning signs, such as does the client want to pay in large amounts of cash? Is the client requesting an unusual shipping route?

The guide then discussed what action cybersecurity companies could take to reduce the risk of misuse at the sales stage, both technical and contractual. For example,

- Narrowing capabilities, very strong permission controls (which limits the people who have permission to use it)
- Use of end user agreements
- Restrictions on re-sale or distribution without notice to the company
- Voiding of warranties if the products are misused.

The guide worked through scenarios in various hypothetical countries and the range of decisions for the company, from refusing the sale to putting in the conditions described above.

As to addressing the OECD Guidelines expectation around remedy, one form of remedy is the prevention of any harm reoccurring. One of the recommendations in the guidance is to put in place a post sale review process, and built into this process some kind of monitoring, both of the situation in country and how the technology is being used. This enables the company to act quickly if something does go wrong and make sure that any new information is fed back into the system.

Ms. Purdon then discussed the example of the Italian surveillance company Hacking Team. Hacking Team has been on the radar of civil society groups for some time, due to its sale of surveillance technology to governments and law enforcement agencies. Its main product is called Galileo, a remote control system which infects a targets

computer or mobile, bypassing encryption, and monitor the target, even turning on a webcam or microphone.

There was suspicion among civil society groups like Citizen Lab and Privacy International that some very intrusive technology was being sold to countries with repressive regimes and a poor human rights record, and it was being used to target human rights defenders, which the company denied. Then Hacking Team were hacked, and information including invoices, client lists, emails were published on the web, which appeared to show that Hacking Team had sold technology to, among other countries, Sudan and Ethiopia, which raised questions about the extent of human rights due diligence undertaken, if at all.

The reason for raising this example was that Hacking Team were not an invisible company, and were able to talk the language of human rights. For example, they have a customer policy, which referred to "know your customer" due diligence, and that raising 'red flags' about a potential customer using the technology to commit human rights abuses. The policy stated the company would "refuse to provide or we will stop supporting our technologies to governments or government agencies that we believe have used HT technology to facilitate gross human rights abuses."

This is the kind of language and commitments expected in a company policy. However, this episode raises questions about the lack of oversight of company practices in this part of the industry. Ms. Purdon referred to earlier comments on the need to verify due diligence, including monitoring and audit assurances – rather than relying on nicely worded policies.

There is also a need to communicate and report on human rights due diligence, but in such a confidential industry, how does that happen? Ms. Purdon also referenced earlier comments about the role of government and the appropriate role of voluntary practices. This case in particular raises questions as to whether it is appropriate for companies in this part of the ICT sector to self regulate in the way they have been.

Ms. Margaret Wachenfeld, Legal Director of IHRB, presented the European Commission *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights,*[40] which was written by IHRB and Shift, and published in June 2013 after 18 months of research and consultation.

It offers practical advice to ICT companies on how to implement the corporate responsibility to respect human rights through step-by-step guidance. Ms. Wachenfeld ran through the chapters of the guides, which reflect each stage of the UN Guiding Principles:

I. Developing a Policy Commitment and Embedding Respect for Human Rights
II. Assessing Human Rights Impacts

[40] http://www.ihrb.org/publications/reports/ict-human-rights-sector-guide.html

III. Integrating and Acting on Potential Impacts
IV. Tracking Performance
V. Communicating Performance
VI. Remediation and Operational-Level Grievance Mechanism

At each step, it summarises what the UN Guiding Principles expect, offers a range of approaches and examples for how to put those expectations into practice, and links users to additional resources that can support their work. The guidance provides examples such as what kind of policies exist in the ICT sector, dealing with government requests, examples on tracking performance, and communicating (transparency reports) and examples of remedy.

At the end of each chapter is a set of questions companies can ask themselves to check they have understood the discussions and completed what is expected.

Conclusions and Next Steps

Mr. John Morrison of IHRB and Mr. Michael Williams of the NCP Steering Board wrapped up the day. A number of specific conclusions regarding next steps are noted as:

- Although the updated 2011 OECD Guidelines do reference Internet freedom, there is a much broader conversation going on around cybersecurity that NCPs who are currently dealing with challenges regarding surveillance and the export of surveillance technology should take note of.

- One of the main strengths of the NCP is starting a dialogue, as NGOs are often unable to reach out to companies and are ignored.

- The UK NCP should have mandatory peer reviews built into the process for each complaint.

- There has been an improvement in transparency over the past few years, including Internet and telecommunication company transparency reports, the Dodd Frank Act[41] and reporting requirements for doing business in Myanmar[42]. But the ICT sector, in particular the sale of surveillance technology, does not look like the kind of sector where transparency is going to lead.

- There had been a lot of work on the knowledge around due diligence, but progress on the *knowing* was not followed by progress on the *showing*. The OECD should explore how to address the need to verify due diligence, including monitoring and audit assurances, and how companies can

[41] http://www.cftc.gov/lawregulation/doddfrankact/index.htm
[42] http://burma.usembassy.gov/reporting-requirements.html

communicate and report on human rights due diligence in such a confidential industry.

- Companies must also explore how transparent they can be. But this is of course a challenge where national security is involved, and can have a knock-on effect as NCPs investigate complaints. This is because any mediation requires transparency, but the issue of mass surveillance is shrouded in secrecy.

- Providing evidence is a big challenge in bringing complaints regarding surveillance as a lot of the information is based on leaked information, which is hard to verify. In addition, the process does not compel the company to disclose certain information. The OECD should look into whether the threshold of evidence is too high in these cases.

- In addition, due to the nature of mass surveillance and the national security element, it is not always possible to identify individual victims that have been harmed. As NCPs are determining whether there had been a violation of the OECD Guidelines, it may not be necessary to identify individuals who have been harmed.

Agenda

09.30) **Opening**

- Mr. Jeremy Carver - UK NCP Steering Board

09:40-11:00) **Panel 1 - An Overview of Key Developments on Human Rights and the ICT Sector relevant to the Application of the OECD Guidelines on MNEs**
This session will cover key developments relevant for companies and NCPs to consider in thinking about the responsibility of MNE in the ICT sector, in particular latest domestic and international cases, reports and standard setting.
Moderator: Mr. John Morrison, IHRB

- Mr. Roel Nieuwenkamp, Chair of the OECD Working Party on Responsible Business Conduct and Professor at the University of Amsterdam
- Mr. Alan Krill, Foreign Affairs Officer, Internet Freedom, Business, and Human Rights Section, U.S. Department of State
- Mr. John Davies, BAE Systems
- Ms. Gabrielle Guillemin, Article 19

Questions and Answers

11.15-12.30) **Panel 2 - Lessons Learned on the Application of the OECD Guidelines in the ICT Sector**
This session will discuss recent cases from the ICT sector brought to OECD NCPs and any lessons learned. The session will discuss the difficulties in bringing a complaint and responding, and key issues that NCPs should be aware of.
Moderator: Ms. Margaret Wachenfeld, IHRB

- Mr. Danish Chopra – UK NCP
- Mr. Malte Hauschild - German NCP
- Ms. Caroline Wilson Palow, Privacy International
- Ms. Kristen Genovese, OECD Watch

Questions and Answers

13.30- 14.45) **Panel 3 - Guidance for NCPs, Businesses and Civil Society on the Responsibility to Respect Human Rights in the ICT Sector**
This panel will discuss key tools and initiatives in the ICT sector that will be a useful source of information and guidance for NCPs.
Moderator: Ms. Lucy Purdon, IHRB

- Ms. Judith Lichtenberg, Executive Director, Global Network Initiative (GNI)
- Mr. John Guelke, EU Surveille
- Ms. Lucy Purdon, ICT Project Manager, IHRB
- Ms. Margaret Wachenfeld, Director of Legal Affairs, IHRB

Questions and Answers

Participants

- Peter Frankental, **Amnesty UK**
- Gabrielle Guillemin, **ARTICLE 19**
- John Davies, **BAE Systems**
- Moira Oliver, **BT**
- Joe Bardwell, **Business and Human Rights Resource Centre**
- Mark Eckstein, **CDC**
- Mark Sun, **Clifford Chance**
- Pavini Emiko Singh, **Clifford Chance**
- Tim Cooke-Hurle, **Doughty Street Chambers**
- Charles Bradley, **Global Partners Digital**
- Judith Lichtenberg, **GNI**
- Hannah Clayton, **Hannah Clayton Consultants**
- Samantha Goethals, **Independent**
- Susan Morgan, **Independent**
- Edward Bickham, **Institute of Business Ethics**
- John Morrison, **IHRB**
- Margaret Wachenfeld, **IHRB**
- Lucy Purdon, **IHRB**
- Adrienne Margolis, **Lawyers for Better Business**
- Owen Larter, **Microsoft**
- Malte Hauschild, **German NCP**
- Florian Schonberger, **Austrian NCP**
- Anne Aarup Fenger, **Denmark NCP**
- Júlia Vágó, **Hungary NCP**
- Joanna Wieczorek, **Poland NCP**
- Danish Chopra, **UK NCP**
- Liz Napier, **UK NCP**
- Jeremy Carver, **UK NCP Steering Board**
- Roel Nieuwenkamp, **OECD**
- Kristen Genovese, **OECD Watch**
- Caroline Wilson Palow, **Privacy International**
- Farnam Bidgoli, **Ranking Digital Rights**
- Tricia Feeney, **Rights and Accountability in Development (RAID)**
- Stephen Lowe, **UK FCO**
- Edward St. John, **UK FCO**
- Christy Hoffman, **UNIGlobal**
- John Guelke, **University of Warwick**
- Alan Krill, **U.S. Department of State**