Comments on the Guidance for the Information and Communication Technologies ("ICT") Sector on Implementing the UN Guiding Principles on Business and Human Rights

General remarks

We welcome the development of the guidelines for the ICT Sector by the Institute for Human Rights and Business (IHRB) and Shift at the request of the European Commission and appreciate the structure of guidance according to the six core elements of the Ruggie principles.

However, we believe that in order to maximise the value of the guidelines, the format can be improved. In order to be fit for practical application, not by for companies but also as practical guidance for users, we believe that the format should be thoroughly revisited – this could be achieved by adding graphics or visualisations for instance. Since these guidelines should also serve as a basis for further constructive engagement with other stakeholders, they should be as clear, usable and accessible as possible.

B. Key concepts

It would be valuable to point out, **under "government violations" on page 8, for example, that the legal framework is far less clear-cut than the current text implies**. States frequently put varying degrees of pressure on businesses to undertake "voluntary" or "self-regulatory" measures as a means of law enforcement online. This leads to actions being taken in a legal grey zone between direct state obligations under international legal obligations, positive obligations of states under relevant legal instruments and the inapplicability of those same instruments to non-state actors.

The approach also leads to jurisdictional and democratic problems when international companies bow to state pressure to impose either political or public relations pressure to implement the law of one country in all countries where they are active. This can be seen in the global implementation of the US Digital Millenium Copyright Act by certain search engines as well as the very un-transparent agreement recently reached in the US with global payment providers to take punitive measures against non-US entities accused of breaching US copyright law.[1]

This often happens in a coercive "do it or we will regulate" environment, where companies can feel obliged to undertake restrictions, where their primary objective will not be to actually address the policy goal (which may be a worthy one), but to pacify their government. This creates an environment where non law-based restrictions are imposed "voluntarily" and effective measures on achieving policy goals (such as fighting child abuse) is replaced with ad hoc and ineffective "voluntary" measures imposed with the goal of pacifying governments seeking a "quick fix". This creates an environment where real problems are addressed with facile "solutions" imposed outside of democratic scrutiny, with collateral damage for human rights.

One example of the severity of this problem is the recent UN Office on Drugs and Crime (UNODC) report on "Use of the Internet for Terrorist Purposes"[2]. This calls for the establishment of "informal relationships or

1 http://www.whitehouse.gov/blog/2012/03/30/safeguarding-america-s-job-creating-innovations
2 http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

European Digital Rights
Rue Belliard 20, B-1040 Brussels
Tel:+32 (0)2 274 2570
E-Mail: brussels@edri.org, http://www.edri.org

understandings with ISPs (both domestic and foreign) that might hold data relevant for law enforcement purposes about procedures for making such data available for law enforcement investigations." This appears to be an unequivocal call by a UN agency that States actively breach Article 17.1 of the United Nations International Covenant on Civil and Political Rights, which states that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence."

Such state interference becomes even more challenging from a business perspective when, as is frequently the case, the calls for "voluntary" cooperation can be manipulated for anti-competitive purposes.

Regarding **Box A d) on meaningful stakeholder consultation on page 10, we believe that the limits of stakeholder consultation should be more clearly defined**. While consultations and dialogues can be useful in some contexts, it must not be promoted as an alternative to democratic decision-making. There are many scenarios where conflicts of interest make it very difficult for businesses, even when starting out with the best possible intentions, to avoid using their position of strength vis-à-vis other stakeholders. The draft also makes the assumption that relevant stakeholder groups will always be present and have the resources to become fully engaged in the processes described. It seems likely that this assumption will frequently not be correct and the draft does not take this into account.

C. Implementing the Responsibility to Respect: Policy Commitment & Embedding

We disagree with the statement on page 12 of the draft that "ICT companies face complex balancing decisions (e.g. in relation to balancing freedom of expression and privacy or child protection)". In reality, business balance a far wider range of concerns - government pressures, public relations interests, unknown variables regarding unintended consequences of taking action in very sensitive areas like child protection and competitive concerns. A "pure" choice (as portrayed in the draft) between, for example, freedom of expression and child protection is a logical impossibility. Furthermore, insofar as a choice has to be made between restricting freedom of expression and any other public policy, this would have to be foreseen by law, following Article 19 of the ICCPR, Article 52 of the Charter of Fundamental Rights and Article 10 of the European Convention on Human Rights. **We propose deleting this paragraph.**

On **page 13, Box 1** on Considering Human Rights in Privacy Policies:

- In order to ensure that privacy policies can be easily understood, we suggest adding examples, such as Mozilla's privacy icons for visual means.
- We suggest linking to a clear explanation not only of the policy but also of the legal situation.
- Companies should also link to their detailed reports on compliance and non-compliance with government requests.
- References to "cookies" should be replaced with references to "tracking technologies" throughout the text, in order to prevent this section from becoming out of date as technologies change.
- The wording on consent is also ambiguous, the tracking/profiling of individuals is invasive and therefore requires active, informed prior consent.
- For a number of reasons, we do not believe that the work of the World Economic Forum deserves to be singled out in the document. For example, the participation in the project does not have an adequate stakeholder balance and its core premise that economic growth and privacy are to be considered in opposition to each other. We therefore suggest deleting the last sentence in Box 1.

D. Implementing the Responsibility to Respect: Human Rights Due Diligence

I Assessing Impacts

Regarding Box 2, on page 19:

- The necessity of an impact assessment prior to the establishment of foreign subsidiaries in order to analyse legislative situation and possible adverse affects on HR resulting from bad legislation should be included in Box 2.

- Regarding the "How", we **suggest to add the development and use of a standardised toolkit** for such impact assessments in order to facilitate such actions by smaller companies and start-ups.

Box 3, on page 21

- Again, a better definition of meaningful stakeholder consultation and engagement is necessary. **We suggest adding a clarification that the goals of such dialogues or consultations should never be misused to circumvent the rule of law or democratic decision-making**.

Box 4, on page 22

- A clearer and better definition of "dual use items" is required. **We suggest a definition in line with Art. 2 of the EU Regulation 428/2009**: "'dual-use items' shall mean items, including software and technology, which can be used for both civil and military purposes".[3]

II. Integrating and Acting – robust responses to government and user requests

Section 3.a on "Possible approaches" appears to overlook completely the clear obligations in international law – Article 52 of the Charter of Fundamental Rights, Article 10 of the Convention on Human Rights and Article 19 of the Covenant on Civil and Political Rights (among others) that make it quite clear that restrictions on freedom of communication must be based on law.

The text is not clear as to whether the "requests from governments" that it refers to are law-based or informal. If the requests are based on an adequate law, then a company has no choice but to respect them, as long as they stay active in that jurisdiction. If the requests are not law-based, then the risk is not just "over-compliance", it is that compliance represents an arbitrary, and therefore illegal, restriction on the freedom of communication of the individual in question.

Box 7 on robust responses to government or user requests (p. 27-28):

- "Government requests" are not clearly defined. We suggest adding a distinction between informal requests and lawful requests.
- A "point of challenge" as described in Box 7 puts the intermediary into the role of judge and jury. If the request is not legally binding, any action on the part of the intermediary is an arbitrary interference. Insofar as non-illegal content is arbitrarily banned by the intermediary, this must be defined very clearly and flagged to users before they start using the service. Furthermore, the potential for unintended consequences must be thoroughly researched. Such (legal) content should only be banned if alternative methods of communication are available. Ex post opportunities to complain about restrictions on freedom of communication are not adequate. Unless there is a clear and urgent reason not to do so, the user should have the opportunity to defend him/herself before any punitive action is taken.
- With regard to government requests, it is surprising the draft only suggests an insistence on agreed legal procedures in relation to cross-border requests. This should be the default response in all circumstances, in order to avoid arbitrary interferences in fundamental rights.
- We suggest highlighting the necessity of disclosing detailed information about requests and information, statistics etc on compliance and non-compliance.

3 Regulation 428/2009 http://trade.ec.europa.eu/doclib/docs/2009/june/tradoc_143390.pdf

- We propose adding a bullet point clarifying that companies should refrain from re-prohibiting illegal activity through their terms of service or contracts. This is necessary to ensure that enforcement of terms of service does not undermine and arbitrarily replace the rule of law. This is particularly important for serious offences.

Box 9 on intermediary liability:

- We suggest to delete “companies are not expected to monitor” since it implies that they could be allowed to do so on a voluntary basis. However, two European Court of Justice cases (C-70/10 and C-360/10) show that pro-active monitoring breaches the right to privacy, freedom of communication & freedom of information. Such breaches do not become less important just because they have been imposed “voluntarily”.
- The reference to “illegal” content is doubly problematic. Firstly, unauthorised copyright content is not illegal, its publication is illegal. Secondly, if a court has not ruled that content is illegal, then it cannot be described as illegal. An accusation is “just” an accusation.
- There is an obvious contradiction by the “ex post” appeal procedures implied by the second last bullet point in box 9 and the dangers of this approach implied in the last bullet point.
- Finally, the distinction between content that is prohibited by law and content that is prohibited by terms of service must be made clear in terms of service. We therefore suggest to add a bullet point that companies should refrain from re-prohibiting illegal activity through their terms of service or contracts.

III Tracking

In Box 13, Tracking Requests for Take-downs, Blocking or Access to User Data:

- We believe that tracking the number of requests is insufficient and therefore propose to add “publishing” to the first bullet point.
- The specific legal basis and notice provider for the takedown needs to be included. We have seen examples, particularly from Germany, of “transparency” that provides virtually no transparency at all. See http://www.chillingeffects.org/notice.cgi?sID=815 , for example.

Box 12, Adverse Impacts on Children in an Online Environment:

- It should be noted that intermediaries can – on their own – only take superficial actions in relation to online child abuse. There is, therefore, a significant danger of unintended consequences of unilateral actions – ranging from interference with ongoing investigations to de-prioritisation of the problem by resource-starved law enforcement authorities.
- Add a bullet point that there also needs to be assessments if the companies' actions do not have adverse affects
- For any mechanism/measures by companies that may impact on users freedom of communication, the standard should always be opt-in and end-user controlled.

IV Communicating

Box 15, on Communicating with Users and about Government Requests:

- As mentioned in section III, the specific legal basis and notice provider for the take-down needs to be included. We have seen examples, particularly from Germany, of “transparency” that provides virtually no transparency at all. See http://www.chillingeffects.org/notice.cgi?sID=815 , for example.
- Similar comments apply regarding Box 15. The specific legal basis must be provided. Copyright holder requests should not, without a domestic legal obligation to do so, lead to removal or blocking of content, as the text in this box appears to imply. Where content is being restricted as a result of a demand by a copyright holder – in full respect of due process and the rule of law – details of which copyright holder made the demand must be made public, unless this was a natural person making a complaint about their own copyrighted material.
- Providers of alleged illegally published content should be consulted upon reception of a request and before any action is taken in order to avoid the disabling or take-down of legal content.

Annex B

Although the table is not meant to be exhaustive, the comment at the intersection of “management of connectivity” and “users/end consumers” misses some elements that need to be included to avoid ambiguity:

1. It is unclear what types of content that is not illegal could be blocked in a rights-friendly environment and what a review process could do to improve the situation.
2. Users/end consumers are not the only injured parties in such circumstances, the person who put the content online, who may not know their content is blocked is also impacted. Furthermore, if the content is not even accused of being illegal, it is not obvious what grounds could be used to appeal the (almost by definition) arbitrary decision of the service provider. Also, if the content is not illegal, there is, almost by definition, no reason for the intermediary to “shoot first (removal/blocking) and ask questions (appeal process) later.”

This table should also contain a reference to provision of personal data to government authorities outside the rule of law and the collection of non-necessary communications data, especially without transparency and explicit consent, is in breach of international human rights norms.

Annex C

Regarding principle 9, we suggest a short preface and modifications as follows:

9. States should provide effective judicial remedies against State or State-corporate or corporate actions that directly or indirectly violate the rights of individuals or groups. In addition, companies should ensure that individuals and communities that are impacted by project activities, but not party to the contract, should have access to an effective non-judicial **corporate** grievance mechanism.