



Association for Progressive Communications
PO Box 29755, Melville 2109
Johannesburg, South Africa
Telefax: +27 11 726 1692

July 18 2012

Consultation on ICT Sector Discussion Paper
Submission to the Institute for Human Rights and Business

Introduction

The Association for Progressive Communications (APC) is an international network and non-profit organisation founded in 1990 to promote and protect the use of information and communication technology (ICT) by all individuals, particularly those living in developing countries. APC's mission is to empower and support organisations, social movements and individuals in and through the use of ICTs to build strategic communities and initiatives for the purpose of making meaningful contributions to equitable human development, social justice, participatory political processes and environmental sustainability.

As part of its "Connect Your Rights! Internet Rights are Human Rights" initiative APC advocates for the recognition of information and communication technology in facilitating human rights; documenting and analysing trends, violations and impacts on freedom of expression, freedom of association and the right to information on the internet at national, regional and global levels. APC also works to build the capacity of women human rights defenders to use the internet safely and securely, facilitating the development of learning and advocacy networks. We appreciate the opportunity to participate in the consultation process provided by the Institute for Human Rights and Business.

Summary

The ICT sector discussion paper provides a good overview of impacts that companies in the sector have in human rights, particularly those relating to freedom of expression. APC supports the recommendations made to develop clear guidelines for protecting and preventing the violation of human rights, particularly in the context of requirements imposed by government and law enforcement agencies. Transparency and engagement with stakeholders, including user groups, is essential to developing these guidelines, and should be considered best practice for all companies.

The discussion paper identifies a number of major challenges faced by companies in the ICT sector, and in particular the tension between government requests and human rights best practices. With reference to this challenge, APC would like to draw attention to the 2011 report from the UN Special Rapporteur on freedom of opinion and expression, which recommended that "any

www.apc.org

Executive director's office / Oficina de la directora ejecutiva
PO Box 29755, Melville 2109, South Africa / Telefax: +27 11 726 1692 / Mail: info@apc.org

determination on what [website] content should be blocked must be undertaken by a competent judicial authority or a body which is independent of any political, commercial, or other unwarranted influences"¹. This recommendation should be considered best practice for both government and business. We advise ICT business, particularly internet intermediaries to be cautious in how "cybercrime" is defined, and strongly recommend that in addition to following good practices when blocking or removing content, companies regularly report on requests for content removal, and their response.

Looking at concerns of privacy, APC strongly recommends that the ICT sector place more focus on issues of online anonymity, and other restrictions to freedom of association, which in turn impacts on freedom of expression. Despite recognition by the Special Rapporteur on freedom of expression that "the right to privacy is essential for individuals to express themselves freely"², including the use of pseudonyms on message boards and chat forums, some governments and corporations have sought to create policies that prevent anonymous monikers online, or require users to register with personally identifying information.

Building on the recommendations for transparency and due diligence made in the discussion paper, we suggest that companies provide a mechanism for dealing with complaints on their website, publishing regular statistical reports on complaints received and their response. An industry ombudsman could also be appointed to deal with specific complaints related to the removal of content and monitoring of internet activity.

With regards to format, we recommend that forthcoming guidance come in the form of regularly updated online resources and reports, which would allow all stakeholders to be kept informed on evolving issues and best practices. Keeping these issues and recommendations in mind, APC sets out its response to specific sections of the discussion paper below.

3.1.1 Blocking, filtering and removing content

APC recognizes that limitations on freedom of expression are permitted in certain circumstances; however those limitations should be in line with the limits of Article 19 of the Universal Declaration of Human Rights, and the three-part test outlined by the Special Rapporteur on freedom of expression in his 2011 report³. Building on this point, we advise internet intermediaries to be cautious in how "cybercrime" is defined. At the May 2012 United Nations' Universal Periodic Review (UPR) of human rights practices in various States, several

¹ Frank La Rue, HRC 17, April 2011 Paragraph 70. <http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/HRC/17/27&Lang=E>

² Frank La Rue, HRC 17, April 2011 Paragraph 53. <http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/HRC/17/27&Lang=E>

³ (1) it must be provided by law, which is clear and accessible to everyone (*principles of predictability and transparency*); and (2) it must pursue one of the purposes set out in article 19, paragraph 3 of the ICCPR, namely (i) to protect the rights or reputations of others, or (ii) to protect national security or of public order, or of public health or morals (*principle of legitimacy*); and (3) it must be proven as necessary and the least restrictive means required to achieve the purported aim (*principles of necessity and proportionality*).

countries made recommendations to ensure that measures to restrict freedom of expression based on cybercrime legislation be based on clearly defined criteria in line with international human rights standards⁴. We recommend that ICT companies be mindful of how national cybercrime legislation adheres to international human rights standards, as well as how these and other policies are discussed within international mechanisms, such as the Human Rights Council and the Universal Periodic Review.

Looking at the discussion of copyright law and internet intermediary liability, APC strongly supports the statement made by stakeholders as to the dangers of placing disproportionate liability provisions on internet intermediaries. There are numerous examples across Europe of internet service providers deleting or blocking content which they fear they could be liable for, based on random criteria. Joe McNamee's report 'Internet Intermediaries: the new cyber police?' in the 2011 edition of Global Information Society Watch provides a critical examination of these cases, and of new trends on intermediary liability and private enforcement. As McNamee states, "[t]he outsourcing of policing of the internet and imposition of punishments by internet intermediaries contradicts basic democratic values and our democratic societies' view of the rule of law"⁵.

3.3 Impacts on the right to privacy

We strongly affirm the need for guidelines to ensure that the ICT industry does not contribute to unlawful and illegitimate violations of right to privacy online. The internet provides new challenges and threats to the right to privacy and freedoms of association and assembly, including increased scrutiny by government and business. As mentioned in the discussion paper, sharing user data with government is a clear violation of privacy, and is often done without legitimate cause. Moreover, new requirements to register personal information to access the internet place users at risk if not properly secured. In 2011, the person details of 13 million South Koreans was leaked online, leading the government to consider new measures to stop online companies from collecting and storing information of users⁶.

Illegitimate surveillance by government, particularly in the case of political or human rights activists is a serious concern in many countries. While APC recognizes that ICT companies are often restricted by license agreements and national legislation, the requirement to cooperate with legal authorities should not preclude companies from responsibility. APC strongly encourages ICT companies to address the ways in which they may be complicit in the violation of rights to privacy, and freedoms of expression and association, following best practices and criteria in line with international human rights standards. Challenges to online anonymity and other threats are outlined in a forthcoming APC report on freedom of peaceful assembly and association on the internet,

⁴ http://www.upr-info.org/IMG/pdf/a_hrc_wg.6_13_l.9_brazil.pdf, http://www.upr-info.org/IMG/pdf/a_hrc_wg.6_13_l.8_india.pdf

⁵ <http://www.giswatch.org/en/freedom-association/internet-intermediaries-new-cyberpolice>

⁶ Kate Jhee-Yung Kim, Lessons Learned from South Korea's Real-Name Policy, Korea IT Times 17 January 2012, <http://www.koreaittimes.com/story/19361/lessons-learned-south-koreas-real-name-verification-system>

which includes recommendations to bodies concerned with human rights instruments⁷.

3.5.1 "Conflict minerals"

APC strongly supports the inclusion of conflict minerals in guidance on human rights in the ICT sector. ICT industry stakeholders should endeavour to increase transparency and accountability throughout the supply chain, in line with the Section 1502 of the Dodd-Frank Act⁸, as mentioned in Section 4.4 of the discussion paper. Voluntary initiatives such as the Extractive Industries Transparency Initiative⁹ can provide support for companies working to uncover the source of the minerals used in production of ICT products.

3.5.2 Impacts related to e-waste

Like conflict minerals, e-waste is an often overlooked consequence of the ICT sector. The ICT sector is one of the fastest growing contributors to waste, with e-waste growing at three times the rate of municipal waste globally¹⁰. The health and environmental costs of e-waste are well documented, and are primarily imposed on developing countries, where much of the global e-waste is dumped, both legally and illegally¹¹. Companies throughout the supply chain should follow best practices of transparency and accountability as to the disposal ICT products, collaborating closely with manufacturers, users, recyclers, government and NGOs to develop sustainable e-waste management systems. One suggestion for increasing accountability has been through the formalisation of labour forces in developing countries that deal with e-waste¹². These and other best practices can be found within the 2010 Global Information Society Watch report on environmental sustainability¹³, which has a specific focus on e-waste, and the forthcoming book 'A practical guide to sustainable IT'¹⁴.

5.1 Embedding respect for human rights in a company

APC strongly affirms the need to embed human rights considerations into every aspect of a company's operations. We support the development of clear guidelines and best practices for ensuring that human rights are respected, and that violations are recognized and appropriately addressed. With respect to the perceived need for clarification about key human rights such as freedom of expression, association and privacy, we recommend that the ICT sector reach

⁷ Comninou, A. (Forthcoming). *New challenges to the freedoms of peaceful assembly and of association on the internet* (Association for Progressive Communications).

⁸ Section 1502, Title XV of the *Dodd-Frank Wall Street Reform and Consumer Protection Act*

⁹ <http://eiti.org/>

¹⁰ <http://www.toxicslink.org/art-view.php?id=134>

¹¹ <http://blog.e-stewards.org/news/un-e-waste-imports-add-to-growing-problem-in-west-africa>

¹² <http://www.giswatch.org/thematic-report/sustainability-e-waste/tackling-e-waste>

¹³ <http://www.giswatch.org/en/2010>

¹⁴ Mobbs, forthcoming.

out to human rights defenders working in the countries where they operate, particularly those focused on internet rights. Strategies for community engagement should be developed, which include human rights networks as well as relevant national and international human rights organisations.

5.2 Assessing risks to human rights

Given the rapid evolution of technology, APC supports recommendations to regularly conduct impact assessments and supplier audits based on update-to-date guidelines and best practices. Civil society, including human rights organizations, should be involved in the process of updating best practices where possible.

5.4 Human rights impacts of business relationships in the sector

While we recognize that telecommunications industry stakeholders are often bound by license agreements with governments, APC recommends that companies be aware of the human rights implications of the license agreement, as well as the legal and regulatory frameworks that exist in the country, prior to signing an agreement. Where regulatory frameworks do not exist, or where they conflict with human rights standards, companies should make governments aware of the standards they follow, to ensure that in an instance where an interception request is received, those handling the request have a well defined procedure to follow.

Focusing on the newly legislated Dodd-Frank Act, APC recommends that the ICT sector lead the movement towards compliance, and view transparency and due diligence as an opportunity to form closer working relationships throughout the supply chain, and to aid in the protection of fundamental human rights.

5.5 Measuring effectiveness of company responses to human rights impacts

APC supports a monthly review of removed content in line with human rights standards, as well as the recommendation made to maintain records in relation to content taken down where criminal allegations are involved. However, we encourage companies to go further by maintaining a record of all requests for content removal and surveillance, in the interest of transparency and accountability to stakeholders and the general public, and publishing these on a regular basis, for example, in consolidated reports identifying the source of the request for take down, the broad nature of content take down requests (for example, under categories such as crime) and surveillance requests (for example, pursuant to lawful warrant, in relation to individuals or organisations).

Further, APC supports the recommendation made that in order to avoid overly censoring content, takedown should be done on a case-by-case basis. Using keyword filtering will unquestionably lead to restrictions of freedom of expression that are not in line with international standards.

5.6 Stakeholder Engagement

APC strongly affirms the need for stakeholder engagement in ensuring the human rights are protected by companies in the ICT sector. This is especially important given the multi-stakeholder nature of internet governance. As

www.apc.org

stressed by stakeholders, it is imperative to make users aware of how and why their online actions may be monitored or restricted, and the recourse available to them. Companies unsure of how to open channels of communication with grassroots organisations and users should look to local ICT actors, such as those within the APC network, for guidance and support. While a pool of 'trusted advisors' may be extremely useful in flagging human rights issues, companies should ensure that these advisors are up to date on relevant UN human rights standards and recommendations, country specific requirements, and are able to connect with reliable sources of information and guidance when needed.

5.7 Complaints handling/grievance mechanisms

On the issue of transparency, while we understand the need to keep some company activities confidential, companies should strive to be as transparent as possible, particularly in the extent to which a company restricts fundamental human rights of privacy, freedom of association and freedom of expression. APC strongly supports the recommendation that companies should notify users that they may be legally monitored according to the laws of the governing state. Moreover, APC recommends setting up industry ombudsmen to deal with rights-related complaints, and suggests that companies link to available complaints mechanisms on their website, and publish statistics annually on complaints received and their response.

We are happy to discuss any aspects of this submission with you. For inquiries please contact Shawna Finnegan: shawna@apc.org

Shawna Finnegan and Joy Liddicoat
Connect Your Rights! Internet Rights are Human Rights
<http://rights.apc.org>

www.apc.org

Executive director's office / Oficina de la directora ejecutiva
PO Box 29755, Melville 2109, South Africa / Telefax: +27 11 726 1692 / Mail: info@apc.org