Freedom of expression and the private sector in the digital age

Submission to the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

Association for Progressive Communications (APC)
April 2016

Table of contents

1. Introduction

The Association for Progressive Communications (APC) is an international network and non-profit organisation that believes the internet is essential for our daily information and communication needs. We advocate for everyone to have affordable access to a free and open internet to improve our lives and create a more just world. We encourage strategies that empower people to use technologies to realise the full range of their human rights, combat discrimination and protect themselves from violence, and to take part in framing policies that govern the use of such technologies, including internet governance discussions, legislation, policy and regulatory proposals.

APC welcomes the focus of the Special Rapporteur on the protection and promotion of the right to freedom of opinion and expression on the responsibilities of the information and communication technology (ICT) sector to protect and promote freedom of expression in the digital age, and the opportunity to contribute to this study.

This submission takes the UN "Protect, Respect and Remedy" Framework and Guiding Principles[1] (hereafter the Ruggie Principles) as the framework for considering the responsibility of the ICT sector in protecting and promoting freedom of expression in the digital age. The Ruggie Principles establish first, that the state has the duty to protect against human rights abuses by third parties, including business; second, that corporations have the responsibility to respect human rights, including by acting with due diligence to avoid infringing on human rights and addressing adverse impacts with which they are involved; and third, that there is a need for greater access by victims to effective remedy, both judicial and non-judicial.

2. Private actors and their impact on freedom of expression

As technology is increasingly pervasive, penetrating a range of aspects of daily life, there is a broad array of private actors whose policies have an impact on freedom of expression in the digital age. There has been significant focus on the impact of large, transnational companies that provide a range of services from search engines and data processors, email and messaging, to social media and news, which certainly deserves the attention of this study.[2] Telecommunications providers and surveillance and cyber security firms are increasingly the subject of scrutiny for their impact on human rights.[3]

We wish to highlight other private actors, who do not typically receive as much public scrutiny, and whose human rights responsibilities are not as well understood:

- **Internet exchange points (IXPs):** IXPs are physical infrastructure through which internet service providers (ISPs) exchange internet traffic among their networks. In some cases they are privately owned and operated, both for-profit and not-for-profit, while in others they are government-run. IXPs channel traffic from many ISPs into one location, so they can be a tempting

[1] Ruggie, J. (2011). Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie. Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework (A/HRC/17/31). www.ohchr.org/EN/Issues/TransnationalCorporations/Pages/Reports.aspx

[2] See, for example, Ranking Digital Rights' 2015 Ranking Digital Rights Corporate Accountability Index: https://rankingdigitalrights.org/index2015; UNESCO's 2015 study, *Fostering Freedom Online: the Role of Internet Intermediaries*: unesdoc.unesco.org/images/0023/002311/231162e.pdf; and the Electronic Frontier Foundation's *Who Has Your Back 2015: Protecting Your Data From Government Requests*: https://www.eff.org/who-has-your-back-government-data-requests-2015

[3] See the Telecommunications Industry Dialogue: www.telecomindustrydialogue.org

target as they offer the opportunity to centralise internet censorship and surveillance. Censorship through IXPs can happen a few different ways. For example, it is possible to install filtering or deep-packet inspection hardware at an IXP, which would mean that packets destined for a censored IP address or containing censored content could be dropped. In addition, the domain name system (DNS) servers that are often located at an IXP could be injected with bad DNS responses, so that when users try to reach a censored domain, they could be redirected to a fake server or receive a message that the domain does not exist.[4] Often IXP-level censorship takes place where IXPs are run by the state, such as in China. However, IXP-level censorship can also happen where IXPs are privately owned.[5] It is important to note that IXPs are not the only location for censorship and surveillance; this sort of inspection or requests for submission of data by governments often happen outside the IXP, and this can be less apparent than at an IXP where the monitoring equipment would be more visible to all parties present at the exchange.

- **Domain registries and registrars:** A domain name registry is an organisation that manages top-level domain names, while a domain name registrar is an accredited organisation that sells domain names for generic top-level domains (gTLDs) to the public. Domain name registries and registrars can be easy targets for law enforcement to threaten with liability if the domains are not removed from or otherwise made unavailable in the domain name system. Often this practice is employed around intellectual property rights and concerns around security and terrorism, but permissible speech, such as political speech and parody, gets restricted as a result. For example, in the UK there is the case of fitwatch.org.uk, in which the police ordered the takedown of domains that were critical of them.[6] To take a more recent example, the website itsnotthetimes.com[7] – a spoof of the New York Times that exposes the U.S. media's biased coverage of Palestinian rights – was removed from the internet in early February 2016 when lawyers for the Times sent Dreamhost, which was hosting the site, a Digital Millennium Copyright Act (DMCA) violation notification. The website is back online, now hosted by May First/People Link.
- **Standard-setting bodies:** The technical standard-setting bodies, such as the Internet Engineering Task Force (IETF), the International Telecommunication Union (ITU) and the World Wide Web Consortium (W3C), develop and promote voluntary standards and protocols for the internet, telecommunications and the World Wide Web, respectively, which may have implications for the exercise of freedom of expression online. To better understand the human rights implications of standards and protocols, a research group has been formed within the IETF-affiliated Internet Research Task Force (IRTF) to increase consideration for human rights in relation to the development of internet protocols, policies and procedures, with the goal of creating human rights guidance for protocol and architecture design.[8] The Human Rights Protocol Considerations Research Group is chartered to research whether standards and protocols can enable, strengthen or threaten human rights, as defined in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights (ICCPR), specifically but not limited to the right to freedom of expression and the right to freedom of assembly.
- **Internet Corporation for Assigned Names and Numbers:** ICANN is a non-profit multistakeholder body responsible for the technical management of internet domain names and

[4]Rodriguez, K. (2016, 14 April). Leaked Documents Confirm Ecuador's Internet Censorship Machine. *Electronic Frontier Foundation*. https://www.eff.org/deeplinks/2016/04/leaked-documents-confirm-ecuadors-internet-censorship-machine

[5]Ibid.

[6]Note, in this case fitwatch.org.uk is registered under a country code top-level domain (ccTLD) and hence to some degree more under government control that gTLDs are.

[7]itsnotthetimes.com

[8]Human Rights Protocol Considerations (HRPC) of the Internet Research Task Force (IRTF). https://datatracker.ietf.org/group/hrpc/charter

addresses. ICANN's policies are directly relevant to a range of human rights, including the rights to freedom of expression and freedom of association, the right to privacy, and cultural rights. For example, decisions around the allocation of domain names and top-level domains may include expressive and communicative elements (e.g. .gay, .sucks, .islam), and as many experts have pointed out, public access to personal information in ICANN's WHOIS database is not fully consistent with international human rights law, which can having a chilling effect on expression for the registration of sensitive domain names. A 2014 Council of Europe report recommended that human rights and the right to freedom of expression in particular need to be fully taken into account when deciding on the approval or refusal of sensitive new gTLDs.[9] The report also found that human rights and the right to private life in particular require a rebalancing exercise with regard to the processing and retention of data under the 2013 Registrar Accreditation Agreement (RAA) as well as to public access to personal information in the WHOIS database. Within ICANN, a Cross Community Working Party on ICANN's Corporate and Social Responsibility to Respect Human Rights has taken on the issue and released a report with practical recommendations for ICANN to respect human rights, by:[10]

- Reviewing its bylaws to ensure they reflect human rights principles
- Setting out in its Human Rights Framework and Principles how human rights principles will be applied to core business procedures and operations
- Approving the revision of its bylaws and its Human Rights Framework and Principles
- Integrating these principles into its Strategic and Operational Plan
- Ensuring that respect for human rights is an ongoing priority for its regular organisational reviews.

The report notes that "implementation of the Guiding Principles is a continuous process of learning and improvement with three core elements: 1) commitment to, and embedding of, the human rights policy; 2) due diligence in following that policy; and 3) remediation procedures for addressing policy violations."

In February 2016, through the efforts of the Cross Community Working Group on Accountability, a group working to enhance ICANN's accountability towards all stakeholders, the ICANN board conditionally agreed to include a commitment to human rights within its bylaws.[11]

3. Pressing legal and policy issues

3.1. Action from the state

As the primary duty bearer for protecting and promoting human rights, the state carries the responsibility to promote and protect human rights, ensuring that companies under its jurisdiction do not commit

[9]Zalnieriute, M., & Schneider, T. (2014). *ICANN's procedures and policies in the light of human rights, fundamental freedoms and democratic values*. Council of Europe. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168048f14f

[10]Article 19. (2015). *Issue report for the Cross Community Working Party on ICANN's Corporate and Social Responsibility to Respect Human Rights: Practical recommendations for ICANN*. https://www.article19.org/data/files/medialibrary/38003/ICANN_report_A5-for-webv2.pdf

[11]The agreed text is as follows: "Within its Core Values, ICANN will commit to respect internationally recognized Human Rights as required by applicable law." This provision does not create any additional obligation for ICANN to respond to or consider any complaint, request or demand seeking the enforcement of human rights by ICANN. "This Bylaw provision will not enter into force until (1) a Framework of Interpretation for Human Rights (FOI-HR) is developed by the CCWG-Accountability (or another Cross Community Working Group chartered for such purpose by one or more Supporting Organizations or Advisory Committees) as a consensus recommendation in Work Stream 2 (including Chartering Organizations' approval) and (2) the FOI-HR is approved by the ICANN Board using the same process and criteria it has committed to use to consider the Work Stream 1 recommendations."

human rights abuses. A key legal and policy issue concerning freedom of expression and the private sector in the digital age is government oversight of internet intermediaries. As a recent UNESCO study found, the operations of internet intermediaries are heavily influenced by the legal and policy environments of states.[12] However, the research findings indicate that state policies, laws and regulations – to varying degrees – are inadequately aligned with the state's duty to facilitate and support intermediaries' respect for freedom of expression.

In fact, rather than fulfilling their obligations under the Ruggie Principles, states often make it difficult or impossible for companies to respect human rights online by imposing legal and regulatory frameworks that are incompatible with the right to freedom of expression as defined under international human rights law. The justification for such limitations comes from constitutions, penal codes, telecommunications regulations, national security legislation, cyber crime and cyber security legislation, and intellectual property rights legislation, among others.

As a result, some states are effectively extending the restrictive environments for freedom of expression that exist offline to the online sphere by enlisting or coercing the private sector. Furthermore, in some cases where states are not preventing companies from fulfilling their obligation to respect human rights, they are failing to act against companies that are operating in ways that limit human rights, thus failing in their duty to promote and protect human rights. In some cases, this is a result of regulatory uncertainty at national level with regards to the obligations of some types of service providers, which is why the Special Rapporteur's report will be extremely valuable.

To provide a few examples of how legal and regulatory frameworks limit the ability of companies to respect freedom of expression online, states:

- Force companies to comply with national legislation, which in some cases is inconsistent with international standards regarding freedom of expression, resulting in the taking down, blocking or filtering of legitimate/protected speech.
- Force companies to turn over personal data to state actors without due process, or simply tap into companies' servers and databases, which can have a chilling effect on speech.
- Force ISPs, in particular mobile telecommunication operators, to implement "kill switches", partial or complete shutdowns of cellular and mobile services and internet traffic.
- Require intermediaries, sometimes through intermediary liability laws, in particular mobile telecommunication operators, to adopt identity verification systems.
- Prevent companies from reporting on takedown requests and transfer of personal data, which provides a degree of transparency in corporate policies. This can mitigate the impact of such policies on freedom of expression, since this reporting would provide users with critical information with which they can make an informed decision on what platforms and services to use.

A few cases we wish to highlight:

- In South Korea, the Network Act requires telecommunications providers to verify users' identity when they subscribe to mobile services regardless of payment method (pre- or post-paid). Other laws, such as the Public Official Election Act, Juvenile Protection Act and Game Industry Promotion Act, oblige intermediaries to adopt identity verification systems. Unnecessary and

[12]UNESCO. (2015). *Fostering Freedom Online: The Role of Internet Intermediaries.* unesdoc.unesco.org/images/0023/002311/231162e.pdf

disproportionate identification of users of internet and mobile services, like SIM card registration, could have negative effects on the freedom of expression and right to privacy of users, especially whistleblowers, human rights defenders, dissidents and social minorities who rely on anonymity for their freedom of expression.[13]

- Another concern is the localising of websites under unclear agreements with the government. In January 2016, YouTube launched country-specific sites for users in Nepal, Pakistan and Sri Lanka. Considering that the government of Pakistan had banned access to YouTube for years, this was welcome news. However, the official communiqué from the Pakistan Telecommunication Authority (PTA) claimed that Google has "promised" to remove any material deemed offensive by the PTA from YouTube, and provided no information to the public regarding the nature of that agreement. It remains unclear whether YouTube/Google is agreeing to remove content in a manner that is inconsistent with international norms.[14]

3.2. Action from private actors

In other cases, ill-designed laws can be abused by private actors to force intermediaries to violate freedom of expression. For example, in the US, the Digital Millennium Copyright Act (DMCA) is regularly used to request ISPs to remove content that is permissible under international human rights norms under the guise of protecting intellectual property rights. The DMCA creates a framework in which most intermediaries would rather comply with all DMCA complaints than face court action, costly legal fees, and potentially huge fines if a court determines that the copyright has been violated. As mentioned with the itsnotthetimes.com example above, DMCA claims including cease-and-desist letters can have a chilling effect and be used to silence legitimate speech, including political speech and parody.

In addition to this being a concern within the US, DMCA claims are being used to censor legitimate expression in other countries. For example, a law firm in Spain has sent DMCA takedown notices on behalf of several Ecuadorian state officials, targeting documentaries, tweets and search results that include images of those officials, alleging copyright infringement.[15] Trade agreements, like the Trans-Pacific Partnership, threaten to perpetuate the mistakes of the DMCA regime and facilitate the censorship of online content through bogus copyright claims in states signatory.[16] In addition, ICANN faces requests from law enforcement agencies for removing domains from the DNS based on copyright claims. Intellectual property interests are pressuring ICANN and influencing policies in such a way that undermines due process and rights.

3.3. Voluntary actions from the private sector

Through their own terms of service and community guidelines, the private sector often takes measures that negatively impact freedom of expression online beyond what is strictly required from them under law. Sometimes this is a result of pressure on internet companies to hand over user information, close user accounts, and remove content, especially in the context of countering violent extremism. This is

[13]Source: Submission of Jinbonet to UN Special Rapporteur David Kaye's call on freedom of expression and the private sector in the digital age.

[14]Bytes for All Pakistan & APC. (2016, 20 January). Call for clarity on terms of lifting of YouTube ban in Pakistan. *APC*. https://www.apc.org/en/pubs/call-clarity-terms-lifting-youtube-ban-pakistan

[15]Sutton, M. (2015, 15 May). State Censorship by Copyright? Spanish Firm Abuses DMCA to Silence Critics of Ecuador's Government. *Electronic Frontier Foundation*. https://www.eff.org/deeplinks/2014/05/state-censorship-copyright-spanish-firm-abuses-DMCA

[16]Malcolm, J. (2015, 17 December). How the TPP Perpetuates the Mistakes of the DMCA. *Electronic Frontier Foundation*. https://www.eff.org/deeplinks/2015/12/how-tpp-perpetuates-mistakes-dmca

especially the case when there are close relationships between companies and governments. In other cases, companies' business models may pose threats to human rights and freedom of expression, such as zero-rating practices.

3.3.1. Terms of service

Terms of service and community guidelines that do not comply with international standards around freedom of expression (the principles of necessity and proportionality) are a significant challenge to freedom of expression in the digital age. For example, Facebook's policy that allows users to flag content has been used to silence unpopular views; its guidelines around nudity have triggered violations of cultural expression;[17] and its real name policy has been used to violate the rights to freedom of expression and privacy of people who rely on anonymity or pseudonyms to express themselves.[18] Furthermore, companies often do not have adequate measures in place to ensure accountability for content removed, or policies in place for remedy. While companies may argue that they have the right to develop community guidelines to shape their platforms according to their own mission and values, when a particular platform becomes so pervasive that users feel that they do not have access to a meaningful alternative, then the need to improve terms of service and community guidelines to ensure that they are compliant with human rights standards is of even more importance.[19]

3.3.2. Countering technology-related violence against women

Given APC's extensive work on the issue of countering technology-related violence against women, we wish to highlight the relevant findings of our research for the Special Rapporteur.

Online harassment, hate speech, stalking, and other forms of online violence against women, LGBTI persons and other users and groups that are most affected by injustice, create a chilling effect and often result in withdrawing from online spaces.[20] At the same time, responses from intermediaries can also create a chilling effect, with terms of service that can lead to censorship by platforms, other users (through reporting), or self-censorship, without actually providing the targets of harassment with redress or recourse, especially for those in non-English speaking countries.

APC conducted research[21] assessing existing company policies to shed light on best practices and possible solutions to women's demands for corporate accountability. A total of 24 in-depth case studies[22] were

[17]See: Russia Today. (2015, 19 April). Brazil to sue Facebook for blocking photo of indigenous woman from 1909. *Russia Today*. https://www.rt.com/news/250961-brazil-facebook-photo-indigenous and Rennie, K. (2016, 16 March). "Nude" Photos of Australian Aboriginal Women Trigger Facebook Account Suspensions. *Global Voices Advox*. https://advox.globalvoices.org/2016/03/16/nude-photos-of-australian-aboriginal-women-trigger-facebook-account-suspensions

[18]An APC flash survey conducted with LGBT activists in 2015 documented that out of 24 respondents, only five used their name as written on their birth certificate, nine used a version of their legal name and nine used a pseudonym. Two thirds of respondents expressed not feeling safe being identified by their real name on Facebook. They cited reasons such as not wanting their family and/or job compromised due to their sexual practices or identity, in addition to "fear of harassment online and offline."

[19]This is especially the case with social media platforms, where the value of the platform is the network it provides, which means that there are fewer comparable alternatives.

[20]APC's research highlights three types of women who are most at risk of experiencing technology-related violence: 1) someone involved in an intimate relationship, 2) professional women, often involved in public expression (activists, journalists, writers, etc.), and 3) survivors/victims of physical assault. See www.genderit.org/onlinevaw/mapping

[21]Athar, R. (2015). *From impunity to justice: Improving corporate policies to end technology-related violence against women*. Association for Progressive Communications. www.genderit.org/sites/default/upload/flow_corporate_policies_formatted_final.pdf#page=38

[22] See www.genderit.org/onlinevaw/countries

documented across seven countries,[23] and the policies of 22 companies[24] were reviewed. Key findings of the research were:

- Recognition of human rights: Only two of the 22 companies reviewed have a formal commitment to human rights.
- National telephony companies: No company reviewed names threats of physical or sexual violence as prohibited behaviour in their terms of service.
- Social media platforms: The companies fail to engage with the perspectives of women outside of North America or Europe.
- Pornography websites: The use of pornography websites for the non-consensual distribution of content is widespread.
- Legal liability: The terms of service are often only a reflection of the company's legal obligations in its country of residence (such as with regard to copyright infringements).

Informed by this research,[25] APC sees a need to move beyond the discussion of liability and towards one of responsibility. Liability denotes a restrictive approach that endangers the free and open nature of the internet and implies a risk-based consideration; responsibility infers a role defined by empowerment, positive action, and leadership. Therefore, we recommend promoting the important role of intermediaries in fostering positive attitudes and accountability online in a way that does not lead to state manipulation or co-option.[26]

This is in line with Article 17 of the Council of Europe's Istanbul Convention, which recognises the important role of social media in reinforcing social and cultural stereotypes as an important contribution to the fight against gender discrimination and freedom of expression of women, who often opt not to participate in public debate due to the misogynistic speech and online harassment they face online.[27] The Convention calls on the private sector to set guidelines to prevent violence against women and to enhance respect for their dignity. It also calls on states to cooperate with the private sector to develop educational programmes for users on how to deal with degrading online content of a sexual or violent nature which might be harmful.

We recommend the following checklist[28] for companies to fulfil their responsibility to respect the right of women to freedom of expression online in the context of online harassment:

1. Does the company have a publicly available statement that stipulates its policy with respect to violence against women?

[23]The seven countries were Bosnia and Herzegovina, Colombia, the Democratic Republic of Congo (DRC), Kenya, Mexico, Pakistan and the Philippines.

[24]The companies reviewed were the following: Social media and networking platforms: Facebook, Twitter, Google+, YouTube, Instagram, WordPress; national telephony companies (telephone, mobile phone, internet services): BH Telecom (Bosnia and Herzegovina), Claro, Empresa de Telecomunicaciones de Bogotá (ETB) (Colombia), AirTel (DRC), SafariCom (Kenya), TelCel, IUSACell, Prodigy (Mexico), Pakistan Telecommunications Company Ltd. (PTCL) (Pakistan), Smart Communications Inc. (SMART), Global Telecommunications Inc. and Philippines Long Distance Telephone Co. (PLDT) (Philippines); search engines and portals: Google Colombia, Microsoft (Bing/MSN Messenger) Colombia, and Yahoo! Philippines; pornography websites: Xvideosm and YouPorn.

[25]This research forms part of a broader research project, "From impunity to justice: Exploring corporate and legal remedies for technology-related violence against women". See: www.genderit.org/onlinevaw/about

[26]Nyst, C. (2013, 26 November). Towards internet intermediary responsibility. *GenderIT.org*. www.genderit.org/feminist-talk/towards-internet-intermediary-responsibility

[27] Council of Europe Convention on preventing and combating violence against women and domestic violence. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168046031c

[28]www.genderit.org/onlinevaw/corporations

2. Does the company engage in meaningful consultation with women, either by soliciting the input of users or by engaging women's rights groups and activists, to understand the potential adverse impacts of its services on women's rights?
3. Is responsibility for addressing issues of violence against women assigned to the appropriate level and function within the company?
4. Do internal decision-making processes enable effective responses to issues of violence against women?
5. Does the company track how effective its responses to issues of violence against women are, either by tracking indicators or seeking feedback from affected stakeholders?
6. Does the company publicly communicate both the occurrence of, and its response to, issues of violence against women?
7. Is there a reporting system in place for women who are adversely affected by violence against women?
8. Does the company consult stakeholder groups on the design and performance of its reporting system?
9. Does the company's reporting system meet the following criteria?
    j. Legitimacy: the mechanism is viewed as trustworthy, and is accountable to those who use it.
    k. Accessibility: the mechanism is easily located, used and understood.
    l. Predictability: there is a clear and open procedure with indicative time frames, clarity of process and means of monitoring implementation.
    m. Equitable: it provides sufficient information and advice to enable individuals to engage with the mechanism on a fair and informed basis.
    n. Transparent: individuals are kept informed about the progress of their matter.
    o. Rights-compatible: the outcomes and remedies accord with internationally recognised human rights.
    p. Source of continuous learning: allows the company to draw on experiences to identify improvements for the mechanism and to prevent future grievances.

3.4. Media concentration and cross-ownership

Over the last decade there has been increasing global media industry consolidation, along with cross-ownership of electronic media production companies with a diverse range of broadband infrastructure and telecommunication operators, as well as with some global retailers, equipment manufacturers and others. Along with this, a series of corporate consolidations are taking place which blur the traditional industry boundaries of these players:

- Mobile and fixed network operators are merging.
- Satellite and cable TV broadcasters are combining and have also become internet access providers.

- Traditional copper cable voice operators now provide broadcast TV and radio channels over broadband.
- Mobile voice operators increasingly provide high-speed broadband and are looking to provide content channels.
- Broadcasters are buying broadband operators, while broadband operators are buying content providers or launching their own in-house operations, as well as making a variety of deals to carry other content.
- Most of these conglomerate media companies are expanding beyond their home borders.

Aside from concerns that horizontal and vertical integration in the electronic media sector limits the diversity of information sources and independence, while restricting the means of distribution to just a few global or regional players, the trends described above are of particular concern in the context of freedom of expression:

1. There appears to be a much more diminished role for public service broadcasting in the new electronic media environment: of what benefit are local content requirements and state-sponsored programming when there are rapidly increasing numbers of “cord cutters” who are less and less likely to access such content? Developing strategies for being able to reach these groups with public service information is becoming an increasingly important priority.
2. There is increasing stratification and inequality in service provision and viewership which leads to isolation and makes it more difficult to reach all of the public in a uniform manner.
3. There are few examples of the adoption of national net neutrality policy frameworks covering cross-ownership and business relationships between infrastructure providers and content producers.

4. Recommendations and useful links for the UN Special Rapporteur's project

APC is pleased that the Special Rapporteur has taken on the important issue of freedom of expression and the private sector in the digital age as an ongoing focus in his mandate.

4.1. Recommendations for the project

To increase the impact and reach of the project, we respectfully share the following recommendations:

1. Conduct regional consultations to gain input from a wide range of stakeholders. Regional internet governance forums, which are held annually in Africa, Asia, Latin America and the Arab region, as well as at the sub-regional level, can provide a useful and relevant platform for such consultations. This will be especially useful for gaining insight into the role of companies that operate at the national and regional levels.
2. Engage NGOs and networks that include marginalised and at-risk individuals and communities who have different experiences and interactions with the private sector with regard to freedom of expression.
3. Link to the work of other UN Special Procedures, as well as human rights mechanisms at the regional level, whose mandates are also impacted by the practices of the ICT industry.[29]
4. Conduct more research on the impact on freedom of expression resulting from media concentration and cross-ownership of content and access provision.

4.2. Useful links

- Global Network Initiative: https://globalnetworkinitiative.org
- Internet Governance Forum Dynamic Coalition on Platform Responsibility: www.intgovforum.org/cms/2008-igf-hyderabad/event-reports/74-dynamic-coalitions/1625-dynamic-coalition-on-platform-responsibility-dc-pr#introduction
- Manila Principles on Intermediary Liability: https://www.manilaprinciples.org
- Ranking Digital Rights 2015 Corporate Accountability Index: https://rankingdigitalrights.org/index2015
- Telecommunications Industry Dialogue: www.telecomindustrydialogue.org/about

[29]Relevant UN Special Procedures include the Working Group on the issue of human rights and transnational corporations and other business enterprises; Special Rapporteur on the rights to freedom of peaceful assembly and of association; Special Rapporteur on the right to privacy; Special Rapporteur on violence against women, its causes and consequences; Working Group on the issue of discrimination against women in law and in practice; Special Rapporteur in the field of cultural rights; Special Rapporteur on the situation of human rights defenders; Special Rapporteur on freedom of religion or belief; Special Rapporteur on the promotion and protection of human rights while countering terrorism; and the Special Rapporteur on the rights of persons with disabilities. Relevant human rights mechanisms at the regional level include the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights; the Special Rapporteur on Freedom of Expression and Access to Information of the African Commission on Human and Peoples' Rights; and the Representative on Freedom of the Media of the Organization for Security and Co-operation in Europe.