APC statement on the Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression to the 32nd session of the Human Rights Council

Association for Progressive Communications (APC)

June 2016

The Association for Progressive Communications (APC) welcomes the report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, which focuses on the critical issue of the role of the information and communications technology (ICT) sector in the promotion and protection of freedom of opinion and expression. Kaye's report, which will be presented at the Human Rights Council on 14 June, is the beginning of a multi-year project that will the key private sector actors and contribute to understanding the main legal and policy issues at stake in relation to how private actors should protect and promote freedom of expression in the digital age.

Kaye's report lays out some of the most critical issues and questions of today. From the private sector's role in expanding access, to regulatory frameworks and the impact of network shutdowns, the report asks important questions about applicable law and the scope of private authority and public regulation. Technology is increasingly pervasive, penetrating a range of aspects of daily life, and there is a broad array of private actors whose policies have an impact on freedom of expression in the digital age. We are pleased that the report catalogues a wide range of private sector actors who together paint a comprehensive landscape of the ICT sector related to freedom of expression: from actors that have received significant focus – large, transnational companies that provide a range of services, search engines and data processors, email and messaging, social media and news – to other actors, such as domain registrars and registries and standard-setting bodies, that do not typically receive as much public scrutiny, and whose human rights responsibilities are not as well understood.

Significantly, the report acknowledges the implications for freedom of expression of technical standards bodies, including the Internet Engineering Task Force (IETF) and Internet Corporation for Assigned Names and Numbers (ICANN), and asserts that standards development often lacks sufficient consideration of human rights concerns.

In addition to state regulation and pressure, the report recognises that companies' own terms of service can violate freedom of expression, especially since they are sometimes unevenly applied, making it difficult to predict with reasonable certainty what kinds of content may be restricted. Echoing APC's findings,[1] the report notes that the world's most popular platforms do not adequately address the needs and interests of vulnerable groups, and that they are reluctant "to engage directly with technology-related violence against women, until it becomes a public relations issue." We encourage the Special Rapporteur to explore this issue further, and refer him to our checklist[2] for companies to fulfil their responsibility to respect the right of women to freedom of expression online in the context of online harassment.

We welcome the Special Rapporteur's commitment to exploring the role of the private sector in expanding access. Given that almost two-thirds of the world is still not online, and that for many more, affordable, high quality access is still elusive, his further work on this issue will make a significant contribution. We particularly welcome the Rapporteur's commitment to paying attention to internet governance frameworks and the need for them to be sensitive to the needs of women, sexual minorities and other vulnerable communities.

[1]Athar, R. (2015). *From impunity to justice: Improving corporate policies to end technology-related violence against women*. Association for Progressive Communications. www.genderit.org/node/4267

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

The Special Rapporteur importantly acknowledges excessive intermediary liability as a threat to freedom of expression, especially when local laws or their implementation are themselves inconsistent with human rights law. Notice and takedown frameworks, like the Digital Millennium Copyright Act of the US, incentivise questionable claims, including those that constitute censorship of political expression, and fail to provide adequate protection for the intermediaries that seek to apply fair and human rights-sensitive standards to content regulation.

Regarding digital security and surveillance, we commend the Special Rapporteur for emphasising again the importance of encryption and anonymity for protecting freedom of expression and opinion, especially for vulnerable groups. He importantly notes that unnecessary and disproportionate surveillance may undermine security online and access to information and ideas, and we encourage him to examine the impact of real name policies in this workstream.

One of the least understood aspects of the business and human rights framework is the right to remedy, and the obligation of the private sector to provide remedial and grievance mechanisms. APC's research[3] found that that remedy mechanisms can be difficult to access in some languages, terms of service are unevenly applied, and violations often are not responded to, which discourages reporting. Since remedy is a responsibility shared by governments and the private sector, the report interrogates the interplay between the two, concluding importantly that "[t]hese questions reflect the uncertainty that human rights victims face in situations where corporate and State conduct are intertwined."

We find the references to the African Declaration on Internet Rights and Freedoms[4] particularly useful, as it can serve as a key tool to promote human rights standards and principles of openness in internet policy formulation and implementation in Africa. We are also pleased to see APC's Code of Good Practice on Information, Participation and Transparency in Internet Governance[5] featured as an example of a civil society initiative oriented to ensure that relevant processes are meaningfully communicated to the public, accountable to all stakeholders, and emphasise democratic participation.

APC appreciated the opportunity to contribute to this timely report, both with written input and participation in a two-day civil society consultation. The Special Rapporteur has encouraged civil society and other stakeholders from less developed countries and vulnerable communities to share their perspectives on these issues. APC looks forward to continuing to contribute to this important project and facilitating input from our community.

Summary of the report

Restrictions to freedom of expression online are a result of state regulation, pressure from the state (even when not strictly required by law), and companies' own policies and terms of service. Kaye's report highlights some key concerns in this area, exploring important questions around how companies respond to government requests and what happens when companies have their own terms of service that go beyond what is required of them by the law.

[3] Athar, R. (2015). Op. cit.

[4] africaninternetrights.org

[5] APC, Council of Europe, & UNECE. (2010). *Code of Good Practice on Information, Participation and Transparency in Internet Governance*. https://www.apc.org/en/node/11199

Among the key concerns contained in the report are those related to *content regulation*, which results in content removal or restrictions based on rationales such as defamation, blasphemy, election-related regulations, harassment or hate speech, incitement, intellectual property, obscenity and indecency, terrorist recruitment or "glorification", the protection of national security and public safety, child protection and the prevention of gender-based attacks. The report points to vague laws and excessive intermediary liability, including the problem of copyright being used for censorship, as contributing to the problem.

Other key concerns highlighted in the report include extra-legal restrictions whereby governments pressure social media companies and other hosts of user-generated content to monitor and take down content on their own initiative and flag content on social media as inappropriate under a platform's terms of service, in order to prompt the company to remove the content or deactivate an account; filtering at various levels, including keywords, websites, or entire domains, which the report warns can raise both necessity and proportionality concerns, depending on the validity of the rationale cited for the removal and the risk of removal of legal or protected expression; network or service shutdowns, which Kaye condemns as "particularly pernicious means of enforcing content regulation"; and network neutrality, including the contentious issue of "zero rating", which Kaye characterises as detracting from the principle of net neutrality, although there is still debate over whether zero-rated services may be permissible in areas genuinely lacking internet access.

With regard to companies' internal policies and practices, Kaye highlights that companies' terms of service are frequently formulated in such a general way that it may be difficult to predict with reasonable certainty what kinds of content may be restricted. He also points to design and engineering choices, noting that the manner in which intermediaries curate, categorise and rank content affects what information users access and view on their platforms. The report concludes that it "remains an open question how freedom of expression concerns raised by design and engineering choices should be reconciled with the freedom of private entities to design and customize their platforms as they choose."

The report also addresses *surveillance and digital security* as key areas of concern in which the private sector plays a central role, as digital communications and data transmitted or stored on private networks and platforms are increasingly subject to surveillance and other forms of interference, whether by the state or private actors. As Kaye highlighted in his previous report to the HRC,[6] surveillance exerts a disproportionate impact on the freedom of expression of a wide range of vulnerable groups, including racial, religious, ethnic, gender and sexual minorities, victims of violence and abuse, children, civil society, human rights defenders, and professionals such as journalists, among others. Other themes in this area he addresses are requests for customer data, sale of surveillance and censorship equipment, covert surveillance, mutual legal assistance treaties and data localisation, and encryption and anonymity.

Kaye identifies *transparency* as an important factor for subjects of internet regulation to meaningfully predict their legal obligations and challenge them where appropriate. However, the report points out that despite multiple reform attempts, there is still a lack of transparency concerning government requests, which threatens the ability of individuals to understand the limits placed on their freedom of expression online and seek appropriate redress when their rights are violated. This is especially the case when it

[6] www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc

comes to transparency around the volume, frequency and types of request for content removals and user data, in particular when the requests come from private actor.

Regarding the right to *remedy*, the report finds that there is limited guidance as to how this should be operationalised or assessed in the context of ICTs. Companies may not always have sufficient processes to appeal content removal or account deactivation decisions where a user believes the action was in error or the result of abusive flagging campaigns. Meanwhile, as noted above, the fact that remedy is a responsibility shared by governments and the private sector leads to uncertainty in situations where corporate and state conduct are intertwined.

Areas for further work

The Special Rapporteur identified the following areas for continued work:

- Restrictions on the provision of telecommunications and internet services: examine the laws, policies and extralegal measures that enable governments to shut down networks or block entire services, and the costs and consequences of such restrictions, as well as the responsibilities of companies to respond to such measures in a way that respects rights, mitigates harm and provides avenues for redress where abuses occur.
- Content restrictions under terms of service and community standards: evaluate the potential of state abuse of private initiatives, the impact of private measures on freedom of expression, and the relevant human rights obligations and responsibilities.
- Liability for content hosting: study the legitimate scope of rationales for content restrictions, the necessity of accompanying restrictions, and the lack of procedural safeguards under existing frameworks for removing third party content; examine sources and modes of intermediary liability in particular contexts and regions and seek to draw out the main principles and practices applicable in order to ensure the ability of intermediaries to promote and protect freedom of expression.
- Censorship and surveillance industry: explore these issues through the human rights framework and encourage due diligence in identifying the uses of such technologies for purposes that undermine freedom of expression.
- Efforts to undermine digital security: identify approaches that could maximise the scope for freedom of expression while nonetheless addressing legitimate governmental interests in national security and public order.
- Internet access: explore issues around access and the private sector, which increasingly seeks to empower the next billions with access.
- Internet governance: pay particular attention to legal developments (legislative, regulatory and judicial) at national and regional levels pertaining to internet governance, keeping in mind the persistent need to maintain or increase human rights participation at all levels of governance, including the setting of technical standards, and to ensure that internet governance frameworks and reform efforts are sensitive to the needs of women, sexual minorities and other vulnerable communities.

Conclusions and recommendations

Although this report is the beginning of a multi-year project, it offers some initial conclusions and recommendations:

- Responding to current, emerging and long-term features of the digital age in relation to the intersections between technology and freedom of expression demands constant analysis and reporting on the impact that ICTs have on the enjoyment of human rights and the active engagement of all stakeholders, particularly from less developed countries.
- Governments also have the responsibility to set viable and effective mechanisms for norm-setting processes and to offer opportunities to the different stakeholders, including civil society, to engage, provide input and participate.
- It is crucial to reinforce the primary responsibility of states to protect and respect freedom of expression offline and online.
- States have the obligation to not pressure the private sector to take unnecessary or disproportionate steps that interfere with freedom of expression.
- The private sector has a key independent role to play to promote and respect freedom of expression online, and to evaluate its practices and take steps towards reinforcing the exercise of the right to free expression, even in adverse contexts for human rights.
- It is imperative that private actors develop and implement transparent human rights assessment procedures that critically review their policies, standards and actions towards determining their impact on freedom of expression and other rights online.