UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Centre for Human Rights
Faculty of Law

Centre for Human Rights, (Special)
For more information, please contact;
Mr. Arnold Kwesiga,
Email: arnold.kwesiga@up.ac.za.

February 23, 2022

CENTRE FOR HUMAN RIGHTS, UNIVERSITY OF PRETORIA STATEMENT ON THE PRACTICAL APPLICATION OF THE UN GUIDING PRINCIPLES ON BUSINESS AND HUMAN RIGHTS (UNGPS) TO THE ACTIVITIES OF TECHNOLOGY COMPANIES – MARCH 7 – 8, 2022

The Center for Human Rights (the Centre) is pleased to participate and issue this statement at the Expert Consultation on the practical application of the UNGPs to the activities of technology companies. The Centre is an internationally recognised university-based institution combining academic excellence and effective activism to advance human rights, particularly in Africa. It aims to contribute to advancing protection and respect for human rights, through education, research and advocacy.

A. General Statement

1. The Centre commends the work of the United Nations and its various organs on the critical milestones made towards the application of legal principles and human rights to the ever changing technology and innovations sector, including Resolution 38/7 on the promotion, protection and enjoyment of human rights on the Internet (A/HRC/RES/38/7), new and emerging digital technologies and human rights (A/HRC/RES/47/23), the right to privacy in the digital age, A/HRC/RES/47/23 on the importance of and ensuring that use of technology is guided by a fundamental respect for human rights and the B-Tech Project and Foundational Papers which provides authoritative guidance and resources for implementing the UNGPs in the technology space. The centre also appreciates the ongoing process of the UN Inter-Governmental Working Group on Transnational Corporations and other Business Enterprises elaborating a legally binding instrument on

business and human rights which will further strengthen the progress already made by the UNGPs.

2. We reaffirm that the corporate responsibility to respect human rights articulated in Pillar 2 of the UNGPs involves varied practices that reflect on the responsibilities of all businesses including technology companies beyond generating profit. Such responsibilities include refraining from harm caused to environment and communities, and positive duties to protect society and environment. This responsibility also extends not only to direct social and environmental impacts of business activity, but also to more indirect effects resulting from relationships with business partners, such as those involved in production and supply chains. This is more relevant to end users of technology companies.

3. As noted by human rights experts, the ever-evolving nature of the technological world affects States in different ways, and addressing these impacts, requires international and multi-stakeholder cooperation in order to benefit from opportunities and to address the challenges arising from this change, as well as bridge the existing digital divide.

4. Specifically, the current African technology landscape comprises technology hubs and incubation centers as its backbone (about 618 of them as of 2019), with most Africans' interaction with technology facilitated by mobile devices. Today Africa makes up 11.6 per cent of the world's internet users with 43 per cent of the continent's population with access to internet leaving many unconnected. Technology is facilitating interconnection of systems and businesses in Africa, especially the financial systems enabled by mobile payment systems—enhancing financial inclusivity.

5. As governments endeavor to adapt their systems to the fourth industrial revolution, it is clear that the question of human rights and technology remains in some instances unanswered, forgotten or intentionally overlooked. Nevertheless, what is evident is that as technology continues to influence social, economic and political transformation of sectors and communities, discussions around the nature, extent and liability for human rights seems to be playing catch up. Key areas around cyber security including access, data protection, freedom of expression and rights to privacy continue to witness rampant abuse with governments grappling with ways of regulating the sector.

B. Addressing human rights risks in business models

6. As experienced globally, new technologies have easily enabled the rapid spread of hate speech, resulting in radicalization, segregation and discrimination—especially of already historically marginalized groups.[1]

7. Many 'social media and search technology' companies have over a long period been accused of using clients' data for business practices that contribute to online and offline human rights harms and grave human rights abuses. Online violence and cyberbullying persists—sometimes in complicit with tech companies. The UN Human Rights Council has noted that such abuses if not addressed could reach extremes such as genocide.[2] Broadly, these human rights abuses limit freedoms of conscience, expression and association which are at the core of any democratic society.

8. Today's climate is filled with uncertainty of online privacy and data breaches involving selling of people's personal data and use in marketing campaigns. Social media's omnipresent surveillance of billions of people poses a systemic threat to human rights and as witnessed in many electoral processes, a threat to democracy. There have been many reported cases of internet shutdowns during electoral processes—limiting free flow and access to information, critical debate and online organizing. Whereas these internet blockades are often initiated by governments, it is also critical to assess the role of technology companies who man and control the tech spaces.

9. The Centre recommends that in line with the UNGPs, States adopt and or review legislation on right to privacy and data protection, on a regular basis, to regulate technology business models profiting from sale of citizens' personal data. The UN HRC has guided that States should ensure that any interference with the right to privacy is consistent with the principles of legality, necessity and proportionality.[3]

C. Human Rights Due Diligence and end-use

10. The Centre reiterates the Human Rights Council resolution (A/HRC/RES/47/23) on the possible benefits of technology in the realisation of human rights and due to the exponential pace at which technological changes, there is need to analyse it in a holistic, inclusive and comprehensive manner for positive leverage.

---

[1] The United Nations Human Rights Advisory Committee, Report on Possible Impacts, Opportunities and Challenges of New and Emerging digital technologies with regard to the promotion and protection of human rights, available here, p 8.
[2] See Report of the Independent International Fact-finding Mission on Myanmar (A/HRC/39/64)
[3] The right to privacy in the digital age : resolution / adopted by the Human Rights Council on 26 September 2019 (A/HRC/RES/42/15)

11. Human rights due diligence helps every technology company address the question, *how does it know that its doing no harm?*. The UNGPS provide approach of using due diligence as a tool to help a company identify, prevent, mitigate and account for any adverse human rights impacts. It will help dissect the argument that 'technologies are morally neutral, and that the responsibility for the adverse consequences of any particular use of technology should be borne by the user,'[4] hence coming up with clear measures to address all actual and potential harm arising in their usage.

12. Recent studies on some of the leading digital platforms show evidence of weak corporate governance and oversight of commitments, policies, and practices affecting internet users' fundamental human rights to privacy, expression, and information despite operating business models reliant on collection and monetization of users' data.[5] In line with the UNGPs, the UN Office for Human Rights guidance on due diligence advises that due diligence for technology companies should involve investigation of actual and potential adverse human rights impacts. This helps mitigate risks to human rights especially where the business models applied offer limited respect for digital rights. It helps a company not only to look at its operations but also those created by any of its business relationships which is a critical angle within tech companies.

D. Accountability and remedy

13. The complexity of the technology sector as; a) fast changing and ever mutating in nature and b) fuelled by an endless string of business relationships creates systems which not only complicate identifying perpetrators of rights violations for accountability but also where and from whom one can access remedy. This technology landscape arguably involves access to personal data for various actors who may not be known to end users and in the instance of data breach, the multiplicity of actors involved often complicates the process of accessing remedy. This has been well expounded on in the State of Internet Freedom in Africa Report 2020 where inadequate regulation and oversight on protection of personal data was highlighted, leading to infringing on individuals' data-privacy rights. These oversights also spread to regulators' abilities to offer remedies to victims.

14. Similarly, the technical complexity and lack of transparency from technology companies leaves people without a good understanding of how technology may affect them and their rights, with a toll on the nature of abuse and the appropriate entity responsible and course of remedial action.

[4] Vivek Krishnamurthy, 'Are Internet Protocols the New Human Rights Protocols? Understanding "RFC 8280 – Research into Human Rights Protocol Considerations"', (2019) 4:1 *Business and Human Rights Journal,* 163-169
[5] 2020 Ranking Digital Rights Corporate Accountability Index, Ranking Digital Rights.

15. Access to information and access to remedy go hand in hand when it comes to technology infringement of human rights. As such states need to strengthened policy and legal framework to enable victims access information as a precursor to remedial action.

E. The State's duty to protect, or regulatory and policy responses

16. Enshrined within the UNGPs and international human rights law, the duty to protect enjoins states to protect against human rights abuse within their territory and/or jurisdiction by third parties including technology companies. The duty requires states to take appropriate steps to prevent, investigate, punish and redress such abuse through effective policies, legislation, regulation and adjudication.

17. However, practical experience has shown many states struggling to limit the extent and reach of technology companies in the areas of privacy and data protection. In the face of increasing citizen awareness and emergency of a strong social media platform as a form of communication, states have resorted to coming up with regulations aimed at gagging citizens digital engagements.

18. Governments have, contrary to their duty to protect and respect human rights, responded to citizen's increased awareness and social media communication and expression avenues by adoption of directives to shut down the internet (internet shutdowns grew by 47 per cent from 2018 to 2019),[6] blocking and or taxation of social media, and enactment of vague or ambiguous law on technology that have been reported to often be weaponised by governments to stifle dissent. Indeed, various sections of Nigeria's Cybercrimes (Prohibition, Prevention Etc) Act, Uganda's Computer Misuse Act, the Kenyan Computer and Cybercrimes Act, and the Malawian Electronic Transactions and Cybersecurity Act are so vaguely worded that they can be weaponized to stifle dissent.[7]

19. These government actions have direct negative impact on human rights.[8] Overarching Governments actions with blanket 'national security and public order' undertones whilst undermining fundamental human rights freedoms and democracy have a huge negative impact in all aspects of the human life for socioeconomic transformation.[9] Such actions are prohibited by the 2014 African Declaration and are contrary to the Human Rights

[6] TARGETED, CUT OFF, AND LEFT IN THE DARK: The #KeepItOn report on internet shutdowns in 2019, #KeepItOn, 2019.
[7] State of Internet Freedom in Africa, Resetting Digital Rights Amidst The Covid-19 Fallout, CIPESA, September 2020.
[8] Life Interrupted: Centering The Social Impacts of Network Disruptions in Advocacy in Africa, Tomiwa Ilori for The Global Network Initiative.
[9] D Mburu Nyokabi, N Diallo, NW Ntesang, TK White & T Ilori 'The right to development and internet shutdowns: Assessing the role of information and communications technology in democratic development in Africa' (2019) 3 Global Campus Human Rights Journal 147-172 https://doi.org/20.500.11825/1582.

Council's call (A/HRC/32/L.20) on states to refrain from measures which prevent access to online information.

20. In case of government requests for user data, telecoms and ISPs, as well as intermediaries such as Facebook and Google, should publish (accessible to the public) details of these requests, providing details including numbers, information given for the requests and action taken by the telecom/ISP/ intermediary (State of Internet Freedom in Africa – SIFA 2016). The publicization of any such requests should always accompany the publication of their privacy and data protection policies.

21. All these notwithstanding, the UNGPs only provide minimum standards of general expectations from business activities in the context of human rights. The Interpretive Guide for Pillar II confirms that 'further work will be needed to develop such operational guidance which will vary depending on the sector, operating context and other factors'.[10] This is especially relevant for technology companies and their activities which are always evolving and may need additional guidance on implementation of the UNGPs. New technologies and business models are putting this framework under unprecedented strain and exposing gaps, conceptual as well as operational – in ongoing responses.[11] Tackling these challenges will require a new commitment to provide more resources to human rights bodies and innovative efforts to conceptualize and comprehensively respond to technological risks.

22. Efficient application of the UNGPs by and to technology companies requires that companies *inter alia*, anticipate and address issues that might occur related to their products and services. The technology industry and the social license and trust issues it faces are global in nature—thus making the international standing and normative nature of the UNGPs a compelling starting point for companies and States seeking to enhance the positive impact and opportunities of technological innovation by doing no harm in all their activities and effectively managing associated risks to people.[12]

23. Several UN human rights Experts, have noted that time has come for States to act collectively to develop an effective international instrument to ensure that businesses take seriously their human rights responsibilities wherever they operate.[13] As such, whereas the UNGPs provide clear articulation of human responsibilities of corporate entities including

[10] The Implementation Guide on Corporate Responsibility to Respect, available here
[11] Report of the Human Rights Council Advisory Committee, Possible impacts, opportunities and challenges of new and emerging digital technologies with regard to the promotion and protection of human rights available here , p 13.
[12] The UN Guiding Principles in the Age of Technology; A B-Tech Foundational Paper
[13] UN OHCHR, Joint Statement by UN human rights experts - UN human rights experts urge States to create a global level playing field for responsible business conduct, (October 19, 2021), accessed at https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=27672&LangID=E.

technology companies, it is important to meaningfully transfer these responsibilities into a binding instrument.

24. All in all, the centre re-echoes the recommendations of the UN human rights experts regarding the importance of a smart mix and that a legally binding instrument adopted at the multilateral level will avoid fragmented approaches to corporate responsibility. The ongoing Open ended Inter-governmental Working Group on Transnational Enterprises and Other Business Enterprises elaborating a legally binding instrument on business and human rights will build on the progress made by the UNGPs.

25. In their current voluntary state, the UNGPs do not impose new legal obligations or change the nature of existing human rights instruments which are being heavily tested by the ever-changing landscape of technology and innovations and corporate influences. There is need for effective binding measures that go beyond articulation of what the human rights instruments mean for both state and corporate entities. It's the only way the challenges and gaps between law and practice will be bridged.