



Call for input to the High Commissioner report on the practical application of the United Nations Guiding Principles on Business and Human Rights to the activities of technology companies

February 2022

About us

Global Partners Digital is a social purpose company dedicated to fostering a digital environment underpinned by human rights. We lead a consortium of civil society organisations from around the world engaged in advocacy work with national governments and with tech companies on business and human rights issues. This work involves leveraging the UNGPs framework as it applies to the tech sector and calling for the incorporation of tech issues in National Action Plans on Business and Human Rights (NAPs). This submission has been prepared with five of these organisations: Asociación por los Derechos Civiles (ADC, Argentina); Blogger's Association of Kenya (BAKE); Institute for Policy Research and Advocacy (ELSAM, Indonesia); Paradigm Initiative Nigeria (PIN); The IO Foundation (TIOF, Malaysia).

Introduction

We welcome the opportunity to respond to the Office of the High Commissioner for Human Rights' call for input to inform the upcoming report on the practical application of the UN Guiding Principles on Business and Human Rights (UNGPs) to the activities of technology companies.

In this response, we provide information and share views on the practical application of the UNGPs to the activities of technology companies, as well as provide input related to the four themes of the consultation. We draw on practical examples and use evidence from our work on business and human rights in the tech sector, where we collaborate with civil society organisations in the global South who engage with their national governments and with tech companies on business and human rights issues. We also provide additional resources in the Annex of this document of our past work in leveraging the UNGPs to promote human rights in the tech sector.

Input Related to the Four Themes

Theme One: Addressing Human Rights Risks in Business Models

The human rights risks associated with the business models of tech companies are receiving increased attention from policymakers, the public and tech companies themselves. We have seen particular concerns being raised over the human rights risks associated with the business models of online platforms, gig-economy services, surveillance companies, and those designing products relying on the massive accumulation of behavioural or personal data or automated tools.¹ As a result, some of the human rights most impacted by tech

¹ See, for example, B-Tech Foundational Paper: Addressing Business Model Related Human Rights Risks, p. 1, p. 4, pp. 10-11.

companies' business models relate to the rights to privacy, freedom of expression, non-discrimination, and to just and favourable conditions of work. At the same time, however, we are also seeing increased awareness of how the nature of online platforms and their business models (often built upon the collection of personal data, maximising engagement, and targeted advertising) are influencing the way people think, suggesting potential impacts upon the rights to freedom of thought and opinion,² an area which remains underexplored.

Too often, however, the UNGPs are only considered when it comes to specific products, policies or decisions of tech companies, with insufficient attention paid to the companies' business models which in and of themselves may create risks to human rights. The corporate responsibility to respect human rights under the UNGPs apply from the moment that the business enterprise is established, meaning that consideration should be given by those involved as to whether the business model itself creates risks to human rights. Rarely, if ever, has this been seen to take place by a tech company, with human rights invariably considered many years into its operations. And we have yet to see tech companies publish or report on human rights assessments of their business models in their entirety, something which should be strongly encouraged.

It is not only the business model of tech companies that requires scrutiny, however, but the related culture and approach that the companies instil. A company whose ethos is to "work fast and break things" is far more likely to create risks to human rights through its products and services than one which places people and societal impacts at the heart of product design and development. A company that seeks to gain a competitive advantage by rushing new products and services to market them first, or which sees data only as a commodity to be used rather than personal and potentially sensitive information, is far more likely to create risks to human rights than one which takes the time to incorporate human rights due diligence and impact assessments into its operations. And a company that relies solely upon its own internal expertise and fails to engage with stakeholders who may be affected by its operations or have relevant expertise (such as civil society organisations, academia and technologists) will more likely create risks to human rights than one that engages in meaningful stakeholder engagement. Unfortunately, these are all aspects of the way we have seen many tech companies operate in recent years.

All of this requires greater clarity over how the UNGPs apply to tech companies that are in the *process* of establishing themselves (as well as developing their culture and ethos) rather than many years into their operations. A more comprehensive assessment of the risks created to human rights by particular business models, as well as how those risks can be mitigated at the very earliest stages of a company's operations, and during its growth, would be beneficial. States and relevant regulators should also look at how appropriate regulatory frameworks can be developed and implemented to ensure that risks to human rights stemming from business models are addressed rather than solely those stemming from very specific products, policies or decisions.

Theme Two: Human Rights Due Diligence and End-Use

Human rights due diligence is a core aspects of the UNGPs. Despite this, little is known about how due diligence is undertaken in practice and incorporated into decisionmaking by tech companies. While we are seeing increasing transparency about human rights impact

² See, for example, Aswad, E., "Losing the Freedom to Be Human", Columbia Human Rights Law Review, 2020, 52(1), pp. 1–66; Alegre, S., "Protecting Freedom of Thought in the Digital Age", Centre for International Governance Innovation, Policy Brief No. 165 — May 2021.

assessments of particular products or services, and how human rights form part of the company's internal governance, public information about the companies' broader human rights due diligence is often highly general in nature.

It is true that tech companies vary considerably in terms of the complexity of their portfolio of products, their types and number of end users and use contexts, and the potential risks associated with their activities, products and relationships. As such, due diligence will look different for different tech companies,³ and there will not be a single way that due diligence should be undertaken. We support the approach recommended in the B-Tech project's Foundational Paper that tech companies implement a principled and transparent approach to prioritising particular products, services, users or user contexts for human rights impact assessment or mitigation, taking into account the severity of potential harms (taking into account scale, scope and remediability) and, if appropriate, the likelihood of the harms occurring (taking into account the nature of the users and the local policy and legal context).⁴

That said, the absence of detailed public information about the way that particular tech companies undertake due diligence at present makes it difficult to assess the extent to which any particular approach is effective. Far greater transparency is needed, and where tech companies lack expertise of human rights risks in a particular context, greater public acknowledgment of this and of efforts to reach out to external stakeholders who do have that expertise would be welcome. In order to avoid duplication of work, tech companies whose due diligence touches upon similar human rights issues, contexts or jurisdictions, should collaborate and undertake joint exercises so that externally sourced expertise, particularly from civil society organisations, can be obtained more efficiently and minimise the demands on those providing information. Larger companies should also work with smaller and medium-sized companies with fewer resources to share their learnings and insight.

The UNGPs recognise that even where companies have not directly caused or contributed to human rights risks or harms, where they are linked to these harms through their business practices or relationships they can and should use their leverage to address them. While we welcome the recognition in the B-Tech project's Foundational Paper that more complex companies and product portfolios will require more extensive and sophisticated risk identification and management systems,⁵ we believe that work could be done to set out explicitly how the scope of responsibilities for linked harms vary according to the scale, power and geographic reach of the company in question. This is particularly important with respect to small and medium-sized tech companies, especially those at an early stage of their operations.

States should also consider how regulation can ensure that proper human rights due diligence is undertaken, while respecting the diversity of business models, human rights risks and resources of companies. The EU's recently proposed Directive on corporate sustainability due diligence provides an example that other states should look to for inspiration.

³ See, for example, B-Tech Foundational Paper: Identifying and Assessing Human Rights Risks related to End-Use, p. 5.

⁴ Ibid., pp. 5-8.

⁵ Ibid., p. 5.

Theme Three: Accountability and Remedy

We support the recommendations of the B-Tech project's Foundational Paper on access to remedy,⁶ and would particularly highlight the points that the paper makes around the need for judicial mechanisms to be at the core of ensuring access to remedy, while recognising that individuals and groups may find it easier and more accessible to use non-judicial and company-based mechanisms when seeking access to remedy. Indeed, there are a number of factors specific to the tech sector which can make judicial mechanisms less appropriate than for other sectors:

- The human rights harms stemming from global tech companies will often affect people in many different jurisdictions, meaning that judicial mechanisms which are limited in their geographic jurisdiction may not be best placed to provide remedies to all affected, not least when national legal and regulatory frameworks diverge;
- Even where a harm is only suffered within a particular jurisdiction, it may still be the case that a large group of individuals are affected, but legal restrictions on standing and group claims may make it difficult for the group that has suffered a particular harm to bring a claim collectively;
- The human rights harms stemming from tech companies may require immediate remediation if remedy is to be effective, whereas judicial processes can be slow and cumbersome;
- As a result of its technical nature and fast-moving evolution, judicial actors may lack a sufficient understanding of technology and its impacts upon human rights to properly evaluate claims made.

For these and other reasons, particular importance must be placed on the responsibilities of tech companies themselves to provide access to remedy, given that they will often be the only actor able to provide a remedy which is timely and effective. We welcome the reiteration in the B-Tech project's Foundational Papers that for remedies to meet international standards they must be timely, proportionate and delivered effectively, and endorse the examples given of potentially appropriate remedial mechanisms, such as compliance hotlines, complaints processes, terms of service enforcement, privacy protections, responsible sourcing alert systems and employee grievance systems.

While states must ensure that their legal frameworks ensure that judicial mechanisms are available for individuals to seek and obtain effective remedies when it comes to the actions of tech companies, they must ensure that the companies are encouraged and able to provide effective remedies as well. We are concerned that many new frameworks regulating online platforms and their activities may in fact undermine their ability to provide an effective remedy. For example, legal requirements to remove particular types of content, especially when only vaguely defined or within tight timelines, put companies in a difficult position if the harm stems from the legal requirement to remove a particular piece of content. Greater attention should be given by policymakers as to how regulation of online platforms specifically - given the rapid development in proposals for regulation - can ensure that companies within scope are encouraged, rather than restricted, in providing access to an effective remedy.

⁶ B-Tech Foundational Paper: Access to Remedy and the Technology Sector: a "Remedy Ecosystem" Approach.

National Action Plans on Business and Human Rights (NAP) are a potential vehicle for embedding the pillar of accountability and remedy into state commitments and company consciousness. The most recent draft of the Nigerian NAP, for example, specifically mentions technology and the ICT sector under the section on "Access to Remedy", particularly in the training of judges on cases involving technology, as a result of the advocacy work of Paradigm Initiative in the country. Similarly, in Malaysia, the IO Foundation has successfully advocated for "technology" to be considered a cross-cutting issue in the country's upcoming NAP Zero Draft, including sections on accountability and access to remedy.

Theme Four: The State's Duty to Protect, or Regulatory and Policy Responses

The B-Tech project's Foundational Papers emphasise the need for a "smart mix" of regulatory measures with respect to the human rights impacts of the products and services of technology companies, including rewards and incentives, accountability and transparency requirements that empower individuals, support and investment in a plurality of business models and extensive guidance for tech companies to follow.⁷ We support this approach.

In practice, however, we are concerned that regulatory frameworks are increasingly patchy and potentially inconsistent in ensuring a high degree of protection for human rights when it comes to the activities of tech companies. For example, we welcome the fact that more countries around the world are developing and implementing privacy and data protection frameworks, a critically essential means for ensuring that tech companies respect their users' right to privacy and can be held accountable when they do not. However, many of those same countries are now introducing new forms of regulation which apply to online platforms and other tech companies, which mandate or encourage the use of surveillance of users' communications and behaviour, restrict the use of encryption and other privacy-enhancing technologies, and require users' data to be localised in the jurisdiction to make it easier for security and law enforcement agencies to access. All of these measures increase the risks to users' right to privacy.

To give another example, many countries are looking at competition law and other measures to enhance the diversity of online platforms and tech companies providing services, thus enhancing opportunities for exercising the right to freedom of expression. Yet many of those same countries are also introducing new forms of online platform regulation that incentivise the over-removal of content, or prohibit broadly and vaguely worded types of content, creating serious risks to the right to freedom of expression.

These challenges may stem from the absence of any holistic approach to the regulation of tech companies in jurisdictions, with particular types of companies and issues regulated in isolation and with different (and often competing) policy goals. Governments should take such a holistic approach, with one opportunity to do being the inclusion of technology and tech companies within National Actions Plans on Businesses and Human Rights, thereby helping to ensure a consistent and complementary mix of measures are taken which apply to the sector.

⁷ B-Tech Foundational Paper: Addressing Business Model Related Human Rights Risks; B-Tech Foundational Paper: Bridging Governance Gaps in the Age of Technology – Key Characteristics of the State Duty to Protect, pp. 6-8.

ANNEX

- **The Tech Sector and National Action Plans on Business and Human Rights**

A guidance document jointly developed by GPD and the Danish Institute for Human Rights that aims to assist state actors and other stakeholders in the development of National Action Plans on Business and Human Rights (NAPs) in the specific context of the tech sector.

<https://www.gp-digital.org/publication/the-tech-sector-and-national-action-plans-on-business-and-human-rights/>

- **Promoting Business and Human Rights in the Tech Sector: Webinar Series**

A four-part webinar series with five modules aims to strengthen the capacity of civil society actors to understand and promote the business and human rights framework in the tech sector – with a focus on privacy and free expression.

<https://www.gp-digital.org/publication/promoting-business-and-human-rights-in-the-tech-sector-webinar-series/>

- **Supporting Tech SMEs to Respect Human Rights: Resource Hub**

As part of our work to support tech companies respect human rights, GPD developed a three-part suite of resources specifically designed for small and medium-sized tech companies.

<https://www.gp-digital.org/event/supporting-tech-smes-to-respect-human-rights-resource-hub>

- **What Options Do Governments Have to Protect Human Rights from Businesses?**

This GPD article sets out the four categories of measures governments can take to protect human rights from business impacts and concluding thoughts and links to resources on effective implementation.

<https://www.gp-digital.org/what-options-do-governments-have-to-protect-human-rights-from-businesses/>

- **National Action Plans: The Importance of Process**

A blog post setting out the ideal four stage process of a NAP development and calling for all NAPs to be developed in an open, inclusive and transparent manner.

<https://www.gp-digital.org/national-action-plans-the-importance-of-process/>

- **Can National Action Plans Make Tech Companies Rights Respecting?**

A blog post discussing the role that NAPs can play in enhancing respect for human rights in the private sector, and the key commitments and safeguards that successful NAPs should include.

<https://www.gp-digital.org/can-national-action-plans-make-tech-companies-rights-respecting/>

- **Can a Business be a Human Rights Defender?**

In this podcast, GPD interviews Michael Samway, former Vice President and Deputy General Counsel for Yahoo! and current adjunct professor at Georgetown University.

<https://www.gp-digital.org/multimedia/in-beta-episode-3-can-a-business-be-a-human-rights-defender/>

- **Data-Centric Digital Rights Principles**

Data-Centric Digital Rights (DCDR) is the advocacy of protecting citizens' rights by transparently implementing the regulations that should protect them. As core stakeholders,

technologists play a critical role as the NextGen Rights Defenders and need to orient themselves through new design and implementation paradigms focused on protecting citizens' digital twins. The DCDR Principles put forward by The IO Foundation are concepts that help them navigate the intricacies of applying Human and Digital Rights in digital infrastructures, products and services.

<https://docs.theiofoundation.org/the-io-foundation/v/data-centric-digital-rights/research/dcdr-principles>