Bridging Governance Gaps in the Age of Technology – Key Characteristics of the State Duty to Protect

A B-Tech Foundational Paper

OVERVIEW

"History teaches us that markets pose the greatest risks—to society and to business itself—when their scope and power far exceed the reach of institutional underpinnings that allow them to function smoothly and ensure their political sustainability."

John Ruggie, author of the United Nations Guiding Principles on Business and Human Rights[1]

Digital technologies can, and in many ways do, improve efficiency and drive economic growth. However, the positive impacts notwithstanding, the dramatic expansion in the use and reach of digital technologies has increased the gap between the scale and impact of technology company business activities, and society's ability to manage any adverse consequences that flow from these. *The United Nations Guiding Principles on Business and Human Rights* (UNGPs) provide a framework for States to bridge such governance gaps.

The framework for State action is set out in the UNGP Pillar I under the heading *The State Duty to Protect Human Rights* which affirms that States should adopt appropriate measures to prevent and address human rights abuses involving business, including technology companies. This duty is anchored in States' existing human rights obligations and elaborates on the legal, policy and other measures States should adopt to protect people from harm.

There is growing recognition—including by States themselves—of the need to develop more effective regulatory and policy responses to the risks associated with digital technologies.[2] An increasing number of States are elaborating policy frameworks at the national and multi-lateral level regarding the development and use of digital technologies such as those based on Big Data, Machine Learning

[1] Special Representative of the UN Secretary-General John Ruggie, A/HRC/8/5, paragraph 2.

[2] UN Human Rights Press release: "'Smart mix' of measures needed to regulate new technologies – Bachelet"

and Artificial intelligence.[3] Other regulatory developments, such as those related to Mandatory Human Rights Due Diligence requirements for companies, may also have implications for how technology companies design, develop and sell products and services. Policy responses to human rights risks related to digital technologies are furthermore beginning to be considered and reflected in some National Actions Plans on Business and Human Rights.[4]

These are welcome developments. But more needs to be done to ensure that human rights are at the heart of State action to protect against the individual and societal risks posed by technology companies, while allowing the enormous potential for positive impact from digital products and services to be realized. The B-Tech project aims to contribute to the field of State policy and practice by exploring and profiling—via multi-stakeholder collaboration—how States should meet their duty to protect against human rights harms involving technology companies.

ABOUT THIS PAPER

This paper is the last of a series of foundational papers published by the B-Tech Project relating to the four B-Tech Focus Areas. These papers are written for stakeholders from across the technology sector, investor community, civil society, and government seeking to understand the key features of the UNGPs as they relate to the tech sector. The series is being released to frame B-Tech engagements and activities aimed at providing normative clarity, guidance, tools and practical recommendations to advance implementation of the UNGPs to address the impacts of new technology products and services on human rights.

[3] Fjeld, Jessica, Nele Achten, Hannah Hilligoss, Adam Nagy, and Madhulika Srikumar. "Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI." Berkman Klein Center for Internet & Society, 2020.

[4] See further "The Tech Sector and National Actions Plans on Business and Human Rights" The Danish Insitute for Human Rights & Global Partners Digital, 2020.

The other papers in the series are available on the B-Tech Portal or can be accessed here:

- *Addressing Business Model Related Human Rights Risks*
- *An Introduction to the UN Guiding Principles in the Age of Technology*
- *Key Characteristics of Business Respect for Human Rights*
- *Identifying Human Rights Risks Related to End-Use*
- *Taking Action to Address Human Rights Risks Related to End-Use*
- *Access to remedy and the technology sector: basic concepts and principles*
- *Access to remedy and the technology sector: a "remedy ecosystem" approach*
- *Designing and implementing effective company-based grievance mechanisms*
- *Access to remedy and the technology sector: understanding the perspectives and needs of affected people and groups*

HEADLINES

1. The State's duty to protect human rights includes protecting against human rights abuses involving technology companies. This is consistent with States' existing human rights obligations, as reaffirmed in the UN Guiding Principles on Business and Human Rights. But States should not, intentionally or otherwise, roll back human rights protections when fulfilling this duty.

2. States should apply a "smart-mix" of the regulatory and policy measures available to them to protect against human rights harms related to the products and services of technology companies, including regulatory measures and accompanying guidance, incentives, and transparency requirements.

3. States should reflect the UNGPs' normative expectation that companies conduct Human Rights Due Diligence related to the impacts of their products and services, in regulation and policies directed at technology companies.

4. Where States financially support, contract with or procure from technology companies, they should actively use that opportunity to ensure that the companies they work with respect human rights.

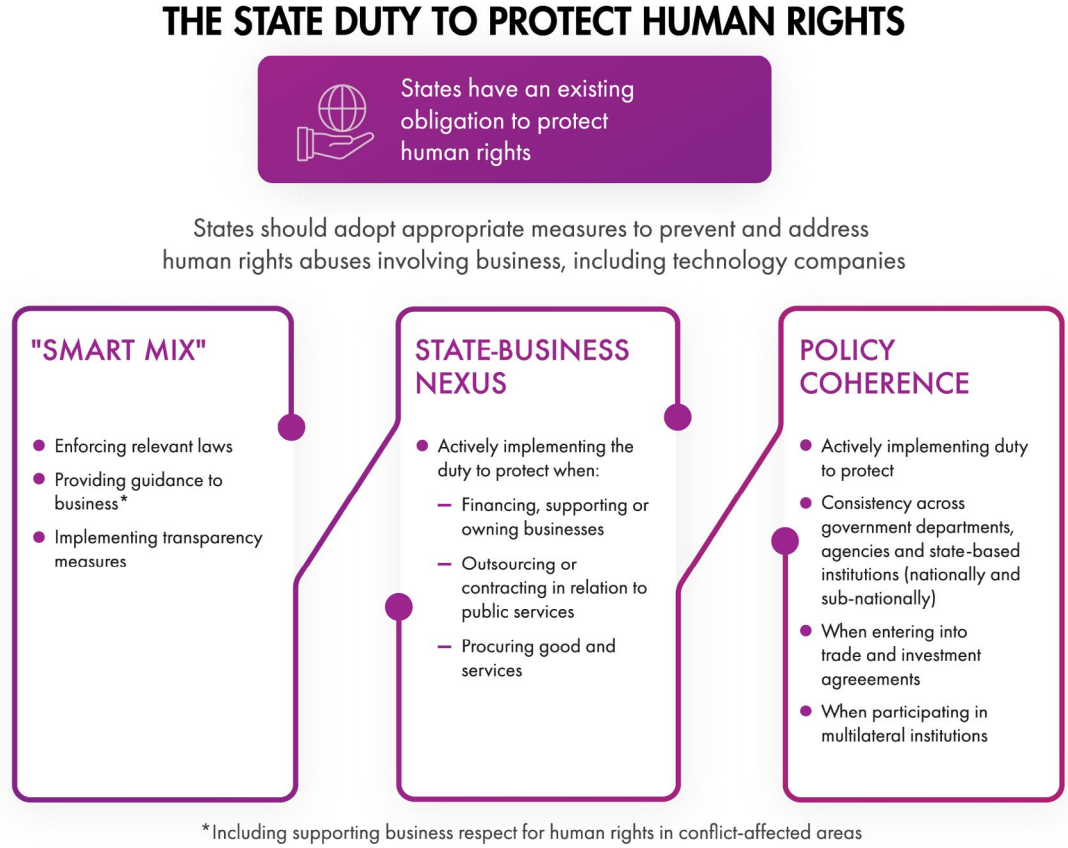
5. States should ensure that they have the necessary policy coherence—as well as capacity and ability—to effectively protect people against harms involving technology companies. The need for policy coherence extends to States participating in multilateral fora and multi-stakeholder processes which are essential tools in ensuring the international legitimacy, coherence and effectiveness of State action.

ONE

The State's duty to protect human rights includes protecting against human rights abuses involving technology companies. This is consistent with States' existing human rights obligations, as reaffirmed in the UN Guiding Principles on Business and Human Rights. But States should not, intentionally or otherwise, roll back human rights protections when fulfilling this duty.

In response to the emergence of data-driven and digital technologies as the predominant engine of early 21st century economic growth, many States around the world have stepped up their engagement with the technology sector. This engagement is multi-faceted, with one key driver being attracting tech entrepreneurs and enterprises to locate and do business within their borders to bolster economic growth, create jobs and pursue development goals. States are often highly active in competing for tech company investment (for example, via tax breaks), incentivizing start-ups, collaborating on research and creating policy frameworks that support domestic innovation.

In parallel to such efforts to maximise the benefits for individual countries of digital technologies and related commerce, a growing number of political leaders have begun to focus their attention on how to address the negative aspects of the digital economy on individuals and society. Fuelled by public concern, specific instances of serious harms, and even calls from within the tech industry itself, more and more States are involved in the development of legislation, as well as ethical guidelines, targeted at specific issues (such as privacy, targeted advertisting practices and cyber-security).



Within this context, the *UN Guiding Principles on Business and Human Rights* provide an authoritative and pragmatic cornerstone for any State action to shape the digital economy. The first pillar of the UNGPs "Protect, Respect and Remedy" Framework re-affirms States' existing duties under international law to protect against human rights abuses by third parties, including business enterprises, and provides a roadmap to guide States in doing so. Business enterprises include technology companies and their activities, products and services.

A key benefit of the UNGPs is that they ground State action in internationally established human rights norms aimed at protecting the fundamental dignity and rights of every individual without discrimination—which should be the focus of any effort to prevent and address human rights risks related to technology. Moreover, it is key to ensuring that digital technologies, and the companies that develop them, are a force for good; addressing human rights harms is a necessary precondition for digital technologies to fully realise their positive potential.

The universality of the norms underpinning the UNGPs increases the chances that technology-oriented State policies and standards can become consistent across geographies, even while the exact form of these will be constructed to meet local realities. This is reinforced by the significant mainstreaming of the UNGPs expectations since their endorsement in 2011, including by international organizations (for example in the OECD's Guidelines for Multinational Enterprises), by States including in the context of regulation, and by investors, civil society and the business community.

A growing number of technology companies are making commitments to operate consistently with the UNGPs, and many are working hard to implement relevant processes and approaches in day-to-day business. Indeed, leading segments of the telecommunications sector have been working to implement their responsibility to respect human rights over several years. Moreover, technology industry associations and professional bodies, as well as institutional investors, National Human Rights Institutions and civil society groups focused on digital technologies regularly advocate for States and companies to act in accordance with the UNGPs. At the UN level, multiple UN reports from appointed experts point to the importance of the UNGPs in their analysis and reporting[5], and the UN Secretary General's Road Map on Digital Cooperation notes that *"There remains a need to address possible protection gaps created by constantly evolving digital technologies. In that regard, the Guiding Principles on Business and Human Rights provide a useful tool. This message is reinforced in the UN Secretary General's Call to Action for Human Rights."*

At the same time, it is imperative that States do not use their obligations to protect against human rights harms as cover to shape company practices, products and services in ways that cause or contribute to human rights violations. In this regard, all stakeholders—especially civil society and human rights organizations—have a crucial role to play in spotting these risks, calling them out and working hard to address them.

[5] See for example reports from the UN Special Rapporteur on the Promotion and Protection of Freedom of Opinion and Expression, e.g. https://www.undocs.org/A/HRC/41/35

TWO

States should apply a "smart-mix" of the regulatory and policy measures available to them to protect against human rights harms related to the products and services of technology companies, including regulatory measures and accompanying guidance, incentives, and transparency requirements.

Growing concern over the human rights risks associated with digital technologies—such as of large-scale infringements on privacy, incitement of violence and ethnic conflict, limiting the ability of civil society to freely express and organise online, and "algorithmic discrimination" (whether in the job market, the criminal justice system or in access to public services)—has turned attention from *whether* States should take action to *how* they should do so.

The UNGPs can, and should, guide all States as they respond to this call for action. They state that in order to meet their Duty to Protect, States should take *"appropriate steps to prevent, investigate, punish and redress human rights abuse through effective policies, legislation, regulations and adjudication"* (UNGP1), and that States *"should consider a smart mix of measures—national and international, mandatory and voluntary—to foster business respect for human rights."* (UNGP3).

The notion of applying a "smart-mix" of measures appropriate to respond to a different range of issues and challenges gains authority from having been embraced unanimously by States and supported by business leaders and civil society when the UNGPs were endorsed in 2011.

Moreover, the "smart-mix" vision is ideally suited to the particular challenges of addressing the wide variety of companies comprising the technology sector; the range and complexity of products, services and solutions that require attention; and the potential of their development and use to infringe on a broad range of civil, political, economic, social and cultural rights. A smart mix of measures—specifically a carefully considered selection of tools designed to foster respect for human rights by tech companies —allows the State to act as a key catalyst to incentivize and drive behavioural change in the very complex and diverse technology sector.

Further, given the scale and cross-border reach of tech companies and the products and services they offer, it will often be necessary to involve a broad range of States to achieve effective coverage and clarity in addressing human rights risks associated with the digital or data-driven economy. The EU General Data Protection Regulation, as well as regulation concerning Platform-to-Business Trading Practices, are examples of such multilateral efforts, as well as the Council of Europe's Convention 108 on Automatic Processing of Personal Data.

There is unlikely to be a single 'silver bullet' solution that will ensure that respect for human rights is consistently placed at the heart of the digital economy. Instead, States will need to explore how to make use of diverse legal regimes and policy domains. In practice, and as outlined by the UNGPs:

- **States should enforce laws that are aimed at, or have the effect of, requiring technology companies to respect human rights, and periodically assess the adequacy of such laws and address any gaps.** In most jurisdictions there are a number of existing laws that can address particular aspects of

human rights risks connected to the technology sector. Beyond the clear relevance of privacy law, data protection and data security, other examples include: labour law that could address adverse impacts of using AI tools in hiring and workplace monitoring; non-discrimination laws might be applied where platforms unintentionally enable discrimination between users; and housing laws have already been used to challenge targeted advertising practices. Consumer law may also prove especially important for certain technology products and services that are user/consumer facing.

In addition to enforcing relevant laws, the UNGPs state that *"It is equally important for States to review whether these laws provide the necessary coverage in light of evolving circumstances and whether, together with relevant policies, they provide an environment conducive to business respect for human rights"* (UNGP3). This includes making sure that "laws and policies governing the creation and ongoing operation of business enterprises, such as corporate law, do not constrain but enable business respect for human rights". This implies that States should ensure that the ability of technology companies to respect human rights is not constrained by legal or regulatory requirements that compel them to act in ways that do not align with international human rights standards, for example when it comes to disproportionate network shutdowns, or restrictions of online content beyond what is permitted by international human rights standards.

- There is no simple formula to ensure that States' regulatory responses will be effective in making technology companies of all sizes, ownership structures and levels of maturity conduct business in a manner that respects human rights. Despite the complexities, States will need to be deliberate and firm in making human rights protections a non-negotiable feature of such laws.
- **States should provide effective guidance to business enterprises on how to respect human rights throughout their operations and in their business relationships.** Even with State policy and regulatory measures in place, companies can benefit from clear direction as to what respect for human rights looks like in practice for their specific part of the technology sector, contexts in which their products and services are sold and deployed or how to take a principled approach to navigating dilemmas.

  While guidance is not prescriptive in nature, it has the benefit of being able to describe best practice, signal what positive outcomes for people should look like, and inform expectations about how companies integrate considerations of affected groups especially those at risk of vulnerability or marginalization (See Commentary to UNGP3). Guidance may accompany regulation, fill near-term gaps in understanding what good corporate conduct looks like, and even be a testing ground for future regulatory proposals.

With regard to the technology sector, issues around which guidance is already available and/or may prove helpful include:

- **Doing business in high-risk contexts:** For example, the UNGPs (UNGP7) identify companies doing business in conflict-affected areas as one situation in which States should actively provide guidance to companies. This includes "home" States playing a role in assisting companies where the "host" State is unable or unwilling to protect human rights. As reflected in a recent report from the UN Working Group on Business and Human Rights,

a portion of the technology sector has products, services and solutions that are used in such high-risk conflict and post-conflict settings. Another example of a high-risk context in which guidance and best practice could be usefully developed are situations in which national law conflicts with international human rights standards.

- **Navigating dilemmas as part of Human Rights Due Diligence:** For example, the *Rabat Plan of Action* can serve a practical tool to combat incitement to hatred, while balancing freedom of expression. It may be necessary, over time, to offer equivalent guidance for other situations faced by different parts of the technology sector (see box on Navigating competing rights).
- **Selling or licensing high-risk products to higher risk customers:** For example, the U.S. Department of State has released Human Rights Due Diligence guidance to assist companies domiciled in the US in seeking to prevent their products or services with surveillance capabilities from being misused by foreign government end-users to commit human rights abuses.

- **States should encourage, and where appropriate require, business enterprises to communicate how they address their human rights impacts.** Governments should consider introducing meaningful reporting and transparency standards to enhance understanding of the workings and risks to people related to digital technologies. As noted by the UNGPs, "State encouragement of, or where appropriate requirements for, such communication are important in fostering respect for human rights by business enterprises. Incentives to communicate adequate information could include provisions to give weight to such self-reporting in the event of any judicial or administrative proceeding. A requirement to communicate can be particularly appropriate where the nature of business operations or operating contexts pose a significant risk to human rights" (Commentary to UNGP3).

State action in this area might focus on:

- **Transparency about specific and severe human rights risks, and the due process needed to respond to these risks**, such as how companies respond to government requests to remove content, suspend social media user accounts or limit/inhibit access or shut-down of telecommunications infrastructure. Transparency initiatives from States in these types of areas will most likely need to be developed via robust multi-stakeholder processes—such as the Global Network Initiative—given the centrality of States to the possible infringement on rights.
- **Transparency related to so-called "black box" phenomenon**, meaning where public knowledge about the ways in which technologies function acts as barrier to mitigating the human rights risks connected to their design and use. It may also be productive for States to focus on companies communicating about how tech business models may exacerbate risks to people or undermine the potential for preventing harms.

- **Transparency regarding Human Rights Due Diligence processes.** An increasing number of States have enacted or are considering legislation with the effect of requiring companies to communicate about the presence and effects of Human Rights Due Diligence policies and systems. A prominent example of this trend is the European Union's Non-Financial Reporting Directive which established that the largest EU listed companies will need to report on human rights risks relevant to their business. Strengthening process-oriented disclosures also serves the purpose of informing better practice within the industry. See *Headline Three* for more on this theme.

Regardless of the focus and substance of State transparency initiatives vis-à-vis technology companies, it is often necessary to establish criteria aimed at maximising the relevance and depth of qualitative reporting, and the comparability of data used in reporting.

Finally, **as States look to apply a "smart-mix" of regulatory measures and policy incentives to protect against human rights harms related to the activities of technology companies, they should be guided by deliberations involving civil society, affected groups, technology companies and other relevant stakeholders.** This will be necessary to navigate the challenges and dilemmas that may arise related to new initiatives, and to better understand how proposals would work in a wide range of real-world scenarios. It is also an important way to reduce the risk that States introduce new legislative or policy measures that are inconsistent with their own international human rights obligations.

Navigating limitations on Rights

States will invariably need to navigate situations where the realization of one right might appear to push against the realization of another right. For example, how should regulators protect individuals and groups against harm from online incitement to hatred and violence, while also protecting the right to freedom of expression? How should States require companies to transparent monitoring of product misuse without increasing the likelihood that those companies will violate privacy rights to achieve this? Such dilemmas are not new for the human rights community and the international human rights framework sets the basic parameters to approach such realities. By way of example, the former Special Rapporteur on the promotion and protection of freedom of opinion and expression has elaborated on this, including in relation to hate speech (A/74/486, para 6.):

> *"Since the freedom of expression is fundamental to the enjoyment of all human rights, restrictions on it must be exceptional, subject to narrow conditions and strict oversight. (…) Any limitations must meet three conditions: (a)* ***Legality.*** *The restriction must be provided by laws that are precise, public and transparent (…)(b)* ***Legitimacy.*** *The restriction should be justified to protect one or more of the interests specified in article 19 (3) of the Covenant (…) (c)* ***Necessity and proportionality.*** *The restriction must be demonstrated by the State as necessary to protect a legitimate interest and to be the least restrictive means to achieve the purported aim. (…)"*

THREE

States should reflect the UNGPs' normative expectation that companies conduct Human Rights Due Diligence related to the impacts of their products and services in regulation and policies directed at technology companies.

THE HUMAN RIGHTS
DUE DILIGENCE PROCESS

The standard of responsibility set out in the UNGPs is that all companies, including technology companies, should "avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved" (UNGP11). An expectation of Human Rights Due Diligence sets the bar beyond a baseline, compliance exercise for companies to conduct one off impact assessments of their activities, products or services. Central to this is the expectation that companies conduct Human Rights Due Diligence to "know and show" how they address adverse impacts that they are, or may be, involved in including from the design and use of their products and services. For further information about Human Rights Due Diligence in the technology, please see *Key Characteristics of Business Respect for Human Rights: A B-Tech Foundational Paper*.

Government agencies mandated to address the impact of technologies on society can, and should, explore ways that State law and policy might incentivize or require technology companies to conduct Human Rights Due Diligence.

State requirements regarding Human Rights Due Diligence by companies can be an important cornerstone of State efforts to foster rights-respecting company conduct, most notably:

- **Spotlighting the importance of internal company governance arrangements in addressing human rights risks:** State efforts should require companies to have in place robust organizational structures, processes and policies to ensure that human rights risks are robustly addressed and internalized in decision-making.

- **Focusing on ongoing assessment and action:** Under the UNGPs, companies must make this assessment and actions ongoing to adapt to new developments (such as unexpected technological breakthroughs or new evidence of product misuse). For more on the distinction between HRIAs and HRDD please see *Identifying Human Rights Risks related to End-Use*.
- **Embeds expectations of engagement and communication:** When implementing HRDD companies will necessarily need to involve relevant internal functions, teams and subject-matter experts. At the same time, the UNGPs place emphasis on the involvement of and communication to, relevant external stakeholders including groups adversely affected by business activities. In a context in which technologies and the workings of technology companies feel opaque to the public and regulators, this feature of HRDD may be especially helpful.

Mandatory Human Rights Due Diligence as part of the "Smart-Mix"

A wave of legal requirements related to human rights due diligence is impacting markets across the world, with Mandatory Human Rights Due Diligence (mHRDD) regimes already in place or in development across a growing number of jurisdictions, including in the European Union. Increasingly, business and investors, alongside civil society organizations, are calling for effective mHRDD legislation. Some business leaders see mHRDD as a way to level the playing field by establishing rules of responsible conduct applicable to all companies, also those who currently lag behind in terms of identifying and addressing human rights risks.

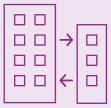
For more information see this OHCHR page Mandatory Human Rights Due Diligence.

FOUR

Where there is a close nexus between a State and a technology company, States should actively use that opportunity to ensure that the companies they work with respect human rights.

A key innovation of the UNGPs is the attention given to the role of a State's economic activities beyond legal and policy measures in shaping the business environment and the conduct of companies. Specifically, the UNGPs note that where there is a close connection between the State and business actors, States should take additional steps to ensure that human rights are protected. Known as the "State-Business nexus" (UNGPs 4-6), this aspect of the UNGPs covers a range of policy areas, including the management of State-owned enterprises, financial and other support provided by States to companies, the privatization of services that may impact human rights enjoyment, and public procurement. The underlying logic is that even where States are operating as economic or commercial actors, "States individually are the primary duty-bearers under international human rights law, and collectively they are the trustees of the international human rights regime". States cannot contract out these duties and must instead take steps to meet them.

When it comes to the technology industry, there are many manifestations of the "State-business nexus" that may provide opportunities to enhance human rights protections and require responsible conduct by tech companies. By way of illustration:



UNGP4 sets out that *"States should take additional steps to protect against human rights abuses by business enterprises that are owned or controlled by the State, or that receive substantial support and services from State agencies such as export credit agencies and official investment insurance or guarantee agencies, including, where appropriate, by requiring Human Rights Due Diligence".*

State-ownership may not be a factor for much of the technology sector but a good number of telecommunications companies around the world are still State-owned. Where telecommunication companies are not State-owned, license agreements structure the relationship between the State and the service providers and can be used to manifest key requirements of Human Rights Due Diligence as part of the State-Business relationship. Some Export Credit Agencies do offer support to technology companies, and the Canadian ECA has embedded requirements in loan agreements with an Indian company to identify and address its human rights risks. With regard to State implementation of this principle, the UNGPs emphasise that "States should encourage and, where appropriate, require Human Rights Due Diligence by the agencies themselves and by those business enterprises or projects receiving their support. A requirement for Human Rights Due Diligence is most likely to be appropriate where the nature of business operations or operating contexts pose significant risk to human rights" (Commentary UNGP4). This includes robust Human Rights Due Diligence requirements for investments by State-owned entities in technology companies, e.g. through pensions funds, as well as for public-private partnerships in development cooperation.

UNGP5 sets out that "States should exercise adequate oversight in order to meet their international human rights obligations when they contract with, or legislate for, business enterprises to provide services that may impact upon the enjoyment of human rights".

This Guiding Principle was drafted to remind states that when they outsource or privatize public services, their human rights obligations cannot be outsourced.

The involvement of technology companies in delivering of public goods is already a major area of human rights concern for many stakeholders including many technology companies. Much of the concern centers on the risk that States use new technologies in ways that abuse human rights. Some contexts in which these concerns have arisen involve programmes to deliver public health, use of surveillance technologies to advance public safety; technologies deployed at borders, and in national defense and national security contexts; and the implications of municipal efforts to develop "smart cities".

At the same time, especially where States contract with companies that have limited or weak Human Rights Due Diligence systems in place, opportunities might exist to raise the bar of

corporate conduct. With regard to State implementation of this principle, the UNGPs emphasize that "As a necessary step, the relevant service contracts or enabling legislation should clarify the State's expectations that these enterprises respect human rights. States should ensure that they can effectively oversee the enterprises' activities, including through the provision of adequate independent monitoring and accountability mechanisms" (Commentary UNGP5).

It is also likely that where a State cooperates with a technology company to deliver a public good, there will be a stronger case for that State to put in place strong transparency requirements such as those outlined above (see reference to UNGP3 in Headline Two "States should encourage, and where appropriate require, business enterprises to communicate how they address their human rights impacts"). Addressing questions related to the statistical evidence about the accuracy and risks of a technological application may be especially important. This could include verifying the representativeness of data and anticipating and mitigating generalization errors. Without checking such elements, statistical issues can lead to the State's use of technologies perpetuating historical and/or large-scale human rights vulnerability.

UNGP6 sets out that "States should promote respect for human rights by business enterprises with which they conduct commercial transactions"

Here, the UNGPs centre on the potential of public procurement as a tool to scale commitment and implementation of business respect for human rights. This may prove a fruitful avenue to advance technology company practice given the reality that States are constantly seeking to upgrade and improve ICT infrastructure and systems.

Deeper examination is required to spot such opportunities while also analysing the risks of encouraging States to shape company practices. In some instances, States could—whether knowingly or unintentionally—use their economic and commercial influence to undercut human rights protections. This has been a topic of concern in relation to State demands on technology companies for access to data and functionality in the context of so-called "track and trace" apps developed to address the COVID-19 global pandemic.

FIVE

States should ensure that they have the necessary policy coherence—as well as capacity and ability—to effectively protect people against harms involving technology companies. The need for policy coherence extends to States participating in multilateral fora and multi-stakeholder processes which are essential tools in ensuring the international legitimacy, coherence and effectiveness of State action.

A key objective of operationalizing the State duty to protect is ensuring coherent policy and action across all State agencies that shape the business practices of, or interface with, technology companies. Where policy coherence is lacking, States will fail to provide technology companies with clear and predictable expectations and undermine both the effectiveness of their own measures, and the ability of technology companies to adjust their practices in a stringent and comprehensive manner.

UNGP8 provides that *"States should ensure that governmental departments, agencies and other State-based institutions that shape business practices are aware of and observe the State's human rights obligations when fulfilling their respective mandates, including by providing them with relevant information, training and support."* This is not a straightforward exercise regardless of the industry sector and range of human rights issues concerned. In the context of technology, challenges for States to overcome will include:

- **Establishing a coherent policy framework, reinforced by political leadership**, that ensures human rights commitments are at the heart of how the States engage with and use a diverse range of technologies. This challenge will be amplified when States have motivations to shape or use technologies in ways that might have repercussions on the human rights protections of citizens at home or abroad.
- **Mapping which agencies are, or can, influence different parts of the technology industry** as well as specific technologies. By way of illustration, an individual sub-set of the tech industry might need the attention of data protection authorities, consumer protection bodies, equal opportunities commissions, public research departments, and multiple parts of government procuring the technology in question.
- **Building internal competence and capability of lawmakers, civil servants, and political leaders**, such that they can navigate the societal and technical complexities of how digital technologies function, the associated risks to people, and the role (including limits) of companies to address these risks. Innovative ideas will be needed to achieve this. For example, the Australian Human Rights Commission has championed the idea of an AI Safety Commissioner, to build capacity in government and industry in relation to promoting and protecting rights when designing, procuring and deploying AI systems.
- **Enable structures for continuous exchange with stakeholder groups to learn about practice-oriented challenges and opportunities of responsible business conduct:** For example, the German government is hosting a consultative inter-ministerial group that includes members from civil society, worker representatives, business and other key stakeholder groups to discuss policy measures and identify best practices by the State to support rights-respecting business conduct. This so-called "National CSR Forum" advises, among others, on the strategy of the development of a National Action Plan for Business and Human Rights in an effort to implement the UNGPs.

Moving digital technology company practices through rights-based investment practices is also a priority challenge for Governments to address, for example by taking practical steps to create an investment environment that allows scanning for human rights issues at each stage of a technology company's lifecycle (See further *Rights-Respecting Investment in Technology Companies, a B-Tech Investor Briefing*).

States must also safeguard domestic policy space to meet their human rights obligations when attracting foreign investment from technology companies or when negotiating trade agreements that include technology. Global data flows underpinning cross-border digital business relationships are an increasingly important element in international trade negotiations, with the free flow of data included in a number of international trade deals. In this context, States should promote respect for human rights in investment and trade agreements, including data protection standards for trade relationships.

The UNGPs were developed in part to address the inter-related phenomenon of a globalized economy, multi-national corporate activity with cross-border implications, and an ever-more complex and rarely static set of value chains. The digital economy and the business activities that underpin it are the latest manifestation of this complexity. Establishing a framework that includes a re-assertion of the role that States must play in their individual capacity is a key value-add of the UNGPs. And yet, it is also clear that many business-related human rights challenges are global in nature and not straightforward to solve.

In light of this, the UNGPs also reinforce the fundamental importance of multilateral and multi-stakeholder approaches to protecting against, preventing and remediating human rights impacts associated with business. The Freedom Online Coalition is a good example of an effort to achieve a multilateral consensus on internet freedoms, e.g. through its joint statement on Artificial Intelligence and Human Rights. The UNGPs note that *"Collective action through multilateral institutions can help States level the playing field with regard to business respect for human rights, but it should do so by raising the performance of laggards. Cooperation between States, multilateral institutions and other stakeholders can also play an important role"* (Commentary to UNGP10).

Collective action must also underpin State action aimed at protecting human rights in the age of the digital economy. There are a number of reasons for this, most notably that:

- State efforts need to recognize that access to, and use of, digital technologies can spread at a speed, scale and depth across borders. This will require large levels of cooperation among States including "by enabling the sharing of information about challenges and best practices, thus promoting more consistent approaches."
- Multilateral efforts might minimize the risks of States pursuing their own, however legitimate - economic and geo-political interests at the expense of building dignity and respect into the heart of the 21st Century digital economy.
- The meaningful involvement of civil society and affected groups, as well investors, academics and business leaders can reinforce accountability for States to prioritize human rights protections, while critically enabling effective ways to address human rights risks associated with digital technologies to be found and implemented.

Whatever the focus, issues and modalities of collective action, the *"Guiding Principles provide a common reference point" and can "serve as a useful basis for building a cumulative positive effect that takes into account the respective roles and responsibilities of all relevant stakeholders." (UNGP10)*

B-Tech

b-techproject@ohchr.org

UN Human Rights invites engagement from all stakeholders across all focus areas of the B-Tech Project. For more information please see the project Scoping Paper. Please contact us if you would like to engage with our work, including if you have recommendations for practical tools, case studies and guidance that will advance company, investor and State implementation of the *UN Guiding Principles on Business and Human Rights* in the business of technology.

UNITED NATIONS
HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

May 2021