HUMAN RIGHTS RISKS IN TECH:

Engaging and Assessing Human Rights Risks Arising from Technology Company Business Models

A tool for **institutional investor engagement** with **technology companies**

B-Tech

UNITED NATIONS
HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

Background and context

Human rights risks in technology company business models

Technology company business models have increasingly come under scrutiny for allegedly creating or exacerbating negative impacts on a range of human rights. Companies from across the sector are being called on to address this concern. Doing so in credible ways is essential to gain (or regain) trust from stakeholders, build resilience into business models, and sustain technology companies' legal and social license to operate.

The UN Guiding Principles on Business and Human Rights (UNGPs) are the leading global standard for preventing and addressing human rights harms connected to business activity. Under the UNGPs, companies are expected to conduct human rights due diligence across all business activities and relationships. This includes addressing situations in which business model-driven practices and technology design create or exacerbate human rights risks. (For further information, please see B-Tech's foundational paper, Addressing Business Model Related Risks).

Addressing business model-related human rights risks may entail different actions by technology companies depending on the scope and tenor of the risks involved. In some cases, direct changes to business models may be necessary to account for especially severe human rights issues. In all cases, companies should take action to prevent, mitigate, and remediate potential and real human rights harms stemming from any of their business model features, i.e., the commercial underpinnings of their business, in accordance with their responsibility to respect human rights under the UNGPs. The present B-Tech tool aims to equip investors to assess companies' progress in discharging that responsibility.

About B-Tech

The B-Tech Project is an initiative of the United Nations Office of the High Commissioner for Human Rights (OHCHR) that provides authoritative guidance and resources for implementing the United Nations Guiding Principles on Business and Human Rights in the technology space.

© United Nations Human Rights Office of the High Commissioner

The role of investors

Institutional investors can have a unique influence over technology companies' governance and decision-making. This influence encompasses companies' efforts to embed respect for human rights into their operations, products, and services. The B-Tech Project has produced this tool to help guide institutional investors' engagement with technology companies on human rights risks linked to their business models ("business model-related human rights risks").

This tool aims to equip investors to (1) accurately assess technology companies' policies and procedures for addressing business model-related human rights risks; and (2) encourage technology companies to adopt approaches to such human rights risks that align with their responsibility to respect human rights.

The tool provides investors with questions to inform their engagement with boards and executives; these questions were developed with input from investors, companies, and civil society. It also embeds a simple evaluation framework to support investors in assessing the quality of company responses received to those questions.

This tool is designed primarily for use in scenarios involving institutional investors investing in technology companies—both public and private—that have surpassed the start-up and early growth stages of the business life cycle. While it is anticipated that institutional investors will be the primary users of this tool, it may also be of value for assessments by regulators and civil society, as well as for self-assessments by technology companies themselves.

B-Tech notes that this tool builds on crucial prior work done by peers at the intersection of investing, technology, and human rights, some of which is referenced in this document.[1] This tool is one of a growing number of resources at this intersection, which together provide important guidance to institutional investors who may be new to applying a human rights lens to their decision-making. The contents of this document are also informed by consultations with civil society organizations, investors, and technology companies. B-Tech thanks all who contributed to the process.

[1] This resource, and in particular the engagement cards and evaluation framework, draw on a number of existing resources developed by B-Tech's peers. These include the Shift Project's *Business Model Red Flags* (see: https://shiftproject.org/resource/business-model-red-flags/red-flags-about/); the Ranking Digital Rights *2020 Corporate Accountability Index* and *2020 Indicators* (see https://rankingdigitalrights.org/index2020/ and https://rankingdigitalrights.org/2020-indicators/); *Navigating the surveillance technology eco-system: A human rights due diligence guide for investors*, from Access Now, the Business & Human Rights Resource Centre, and Heartland Initiative (see https://www.accessnow.org/cms/assets/uploads/2022/03/2022_STAP_Guide.pdf); the Shift Project's *Leadership and Governance Indicators of a Rights Respecting Culture* (see https://shiftproject.org/resource/lg-indicators/about-lgis/); and Ranking Digital Rights' *It's the Business Model* (see: https://rankingdigitalrights.org/its-the-business-model/).

© United Nations Human Rights Office of the High Commissioner

B-Tech

Why should investors focus on business models?

Focusing on human rights risks linked to company business models delivers considerable utility for investors, who often have limited opportunities to engage investee companies on human rights issues. This is because:

- Without board and top leadership engagement to mitigate risks and adapt business models to prevent future human rights harms, human rights risks that flow from a company's business model are likely to be reproduced, even where internal human rights policies, processes, and programs exist.
- By contrast, evidence that the board and top leadership are engaged in addressing business model-related human rights risks is a strong signal to investors that a company takes its responsibility to respect human rights seriously, and thus is likely to be anticipating other risks and impacts.
- Where a company fails to address business model-related risks, this can result in significant threats to a company's social, and even legal, license to operate, creating knock-on financial and other risks for investors.
- Engaging directly with a company on business model-related risks allows investors to better understand the policies and processes adopted by the company in respect of some of its most serious human rights risks. This includes the nature of mitigation processes in place and the extent to which the company has taken a role in enhancing pathways for remedy.

Defining business models

The B-Tech Project is using the term "business model" to denote "the value a company seeks to deliver, and to whom, and how it delivers that value in the pursuit of commercial success". This draws on two complementary ways of understanding business models that help bring focus to their crucial role in business respect for human rights:

1. Business model choices substantially influence day-to-day business practices: Business model choices are made and reviewed by the top leadership of an enterprise responsible for strategy. Executives and senior managers then work to ensure that these strategic choices are reflected in the company's operating model. Where this leads to business processes, incentives, and practices that increase risks to workers, communities, or consumers, a tension arises between a company's business model and its ability to respect human rights.

2. Business models are made up of three elements, all of which can create human rights risks:

- **A Value Proposition:** What the company offers and to whom. For technology companies this includes the products, services, insights, or solutions the company delivers to customers, and who those customers are.

© United Nations Human Rights Office of the High Commissioner

- **A Value Chain:** How the company delivers value and who or what it relies on to do so. For technology companies this includes how they source, treat, and use data.
- **A Revenue and Cost Reduction Model:** How the company generates financial income or minimises costs in order to be profitable.

As B-Tech has previously noted in its foundational papers, "when considering the impacts of digital technologies, … it is mostly in their use that human rights harms will manifest." With that in mind, this tool is primarily concerned with end-use human rights risks associated with digital technology products and services. It should be noted that while "end-use" refers to the ways in which products and services are ultimately used by customers and end-users, end-use-related human rights harms may themselves originate in various areas of company business models (in sales channels, research and design processes, etc.).

© United Nations Human Rights Office of the High Commissioner

B-Tech

Institutional investor engagement tool

Tool structure

Engagement cards

This tool provides a series of "engagement cards" for investors to use in modeling their engagement with technology companies. Each card is a self-contained guide to engaging companies on a discrete issue connected to business model-related human rights risks. Each card includes an **overview of the importance of the issue and a list of engagement questions for investors to ask of companies**.

The tool includes five such engagement cards; Card 1 pertains to issues of business model governance and Cards 2-5 pertain to specific features of technology company business models that B-Tech has identified as potentially carrying elevated human rights risks.

Evaluation framework

This tool also provides an evaluation framework to be used by investors in evaluating the quality of company responses to engagement questions. The framework follows the same structure for each engagement card. The table below demonstrates the structure and content of the evaluation framework and provides a short explanation of the logic applied.

© United Nations Human Rights Office of the High Commissioner

LESS STRONG

STRONGER

Response level		Explanation
-1	**Red Flag** – The company contests the relevance of the question without any clear explanation, and/or simply states that it is unable to provide responses, and/or states that it does nothing illegal.	The first two levels pertain to scenarios in which investors receive responses to engagement questions indicating that a company has no processes in place to assess and act on the business model-related human rights risks raised by the question.
0	**Absent** – The company recognises the relevance of the question but states that it does not currently have any practice in place to address the issue.	
1	**Nascent** – The company describes a regular process with this aim – and provides at least one example from the past 12 months.	Levels 1 through 5 in this evaluation framework reflect points emphasised by experts during consultations on earlier drafts of this tool. These include that: – Examples to substantiate descriptions of processes are critical for investors seeking to ascertain the seriousness of a company's engagement on business model-related risks. – Investors and civil society organisations put significant stock in evidence of open engagement by a company with diverse internal and external stakeholders, and less in evidence of a process or management system merely existing.
2	**Developing** – …AND the company describes how actions from this process are assigned and resourced – and provides at least one example from the past 12 months.	
3	**Good** – …AND the company describes how the board/company is informed by the perspectives of internal stakeholders—including the nature of input provided by teams responsible for human rights, sustainability, etc.—and provides at least one example from the past 12 months.	
4	**Excellent** –…AND the company describes how the board/company is informed by the perspectives of both credible external experts and affected stakeholders (or proxies for affected stakeholders, such as human rights defenders or organisations working on behalf of affected individuals or communities) – and provides at least one example for each category from the past 12 months.	
5	**Leading** – …AND the company publicly discloses its practices and/or plans across all prior levels, including progress and challenges in implementing these practices; number and nature of grievances received, and; processes in place for providing remedy to adversely impacted individuals and/or communities.	

© United Nations Human Rights Office of the High Commissioner

B-Tech

Engagement on business model governance (Card 1)

The first card in this toolkit is not specific to an individual business model feature; rather, it is designed to inform investors' engagement with company boards and executives regarding whether company leadership actively reviews and engages as necessary with the company's business model-related human rights risks broadly. The questions included in this card are primarily designed to be addressed directly to boards and senior leadership teams. This card can be used by investors when engaging companies in any part of the technology sector. Responses to the engagement questions included in this card should be assessed using the evaluation framework provided above.

CARD 1

Engaging boards and executive teams on business model-related risks

OVERVIEW OF THE ISSUE

Regular engagement by boards and executives with business model-related human rights risks suggests that leadership views these risks as relevant to the fiduciary duty of board members to the company and shareholders. When this is the case, it is more likely that senior leadership will support assessments, controls, and actions to identify and address business model-related human rights risks. Without board and executive engagement—even where human rights or ethical use policy commitments, processes, and teams are in place—it is unlikely that a company's strategy and business model-related practices will be scrutinised for human rights harms to the same extent.

ENGAGEMENT QUESTIONS

Do the board and executive team…

1. Evaluate the human rights risks associated with the company's main source of revenue or market valuation?
2. Evaluate the human rights risks of strategic decisions and new ventures?
3. Identify and address top management performance incentives that risk promoting behaviours that undermine respect for human rights?
4. Ensure that the company has in place specific plans and processes to raise, assess, and mitigate harms associated with the most severe potential human rights risks connected to the use of its products and services?
5. Review and approve all company political engagement activities to ensure that the aims of such engagement do not introduce or exacerbate business model-related human rights risks?

© United Nations Human Rights Office of the High Commissioner

Engagement on business model features (Cards 2-5)

Cards 2-5 are intended to support investor engagement on specific features of technology company business models that B-Tech has identified as potentially carrying human rights risks. Each of the four subsequent cards discusses one such business model feature in detail. These four features are not present in the business models of all technology companies; rather, the four business model features included in this tool were selected based on their prominence in the technology sector and their links to heightened human rights risks. They are:

- Algorithm-supported decision making
- High-risk customers or end-users
- Conflict-affected and high-risk areas
- Low-leverage sales practices

These are not the only features of technology company business models that carry human rights risks; there are numerous others that may heighten the risk of human rights harms. Examples may include offering products or services whose overuse can negatively impact users' rights (particularly vulnerable populations) or using data collection and retention practices that may imperil the right to privacy. This tool's in-depth discussion of the four business model features below is meant to act as a template for investors to structure their engagement with technology companies on other business model features that may carry human rights risks.

Unlike the engagement questions in Card 1, the engagement questions in Cards 2-5 do not relate exclusively to the activities of boards and senior leadership teams, and may be addressed to various relevant senior individuals within an organisation who have oversight or direct knowledge of the specific business model feature in question.

The engagement questions on Cards 2-5 all follow the same template, with references to the relevant business model feature inserted. Responses to these engagement questions should be assessed using the evaluation framework provided above.

© United Nations Human Rights Office of the High Commissioner

CARD 2

Algorithm-supported decision making

For use when a company's commercial success depends, in part or in full, on the development and/or use of machine learning algorithms to make decisions that may materially impact human rights.

OVERVIEW OF THE ISSUE

In many cases, machine learning algorithms are used by companies to optimise or otherwise facilitate their operations in ways that do not pose risks to human rights. However, the use of algorithmic technology can also be linked to risks of real and potential human rights harms. These risks are present across the technology sector and arise where algorithms are used to generate predictions and/or recommendations that, when implemented (especially without human oversight or intervention), negatively impact the rights of individuals and/or communities.

In some cases, this occurs through instances of algorithmic bias, wherein algorithmic outputs unintentionally lead to decisions that adversely affect groups based on characteristics such as ethnicity, gender, sexual orientation, religion, criminal history, family status, etc. This type of bias can result from the use of training data that is incomplete, unrepresentative, or inclusive of inappropriate features or data points, or from errors in the design of decision algorithms themselves, for example.

The use of algorithm-supported decision making has been implicated in instances of alleged unintentional machine bias, for example in mortgage approval or healthcare allocation decisions. When government agencies use this technology to make decisions, risks to individuals and communities can be amplified and consequences can be especially serious. Examples of such potential impacts include where machine learning is used to make decisions about criminal justice or government assistance programs.

Regardless of the level of bias present, machine learning algorithms do not predict with 100% accuracy. This becomes more problematic when machine learning algorithms are used to make decisions that directly impact people—resource allocation decisions in hospitals, for example. In these scenarios, additional human rights risk may be introduced, especially if algorithmically-driven decisions are implemented without human oversight.

In other cases, algorithms designed to deliver recommendations for optimising a specific metric may result in decisions with unforeseen negative consequences for human rights. For example, some contend that social media content recommendation algorithms that prioritise driving users toward the most "engaging" content have instead surfaced

© United Nations Human Rights Office of the High Commissioner

extreme or "borderline" content— which has been described as especially engaging for social media users. Accordingly, such algorithms have been accused of contributing to online extremism.

Some social media platforms have taken steps to de-prioritise extreme or borderline content or to increase transparency around how borderline content is defined. However, some observers argue that greater transparency around algorithms in general—including content recommendation systems—is needed, and that algorithmic design should be subject to safety review by independent regulators in a manner that allows for risks to be understood and assessed. This is a complex task, especially given that the inner workings of some machine learning techniques inherently cannot be interpreted. Nevertheless, this complexity should not obviate the need for independent review; the business responsibility to respect human rights applies equally even when the technology in question is especially complex.

ENGAGEMENT QUESTIONS

1. Does the board consider, as part of its decision making, risks to human rights associated with use of the company's algorithm-supported decision making?
2. Does an executive oversee regular assessments of privacy and discrimination risks associated with use of the company's algorithm-supported decision making, while also ensuring that these assessments are conducted in a credible and independent fashion?
3. Does the company take steps to mitigate risk to human rights associated with use of the company's algorithm-supported decision making? Examples of action could include internal controls and escalations, bias training and human rights training for internal algorithm developers and users, regular testing/modifying of its algorithmic systems, technological safeguards, contractual safeguards, or capacity building for customers or end-users.
4. Does the company collaborate with relevant stakeholders, peer companies and/or experts to mitigate systemic risks to human rights associated with use of the company's algorithm-supported decision making?
5. Does the company take preemptive steps to provide or increase access to remedy for individuals that are exposed to the most severe human rights risks associated with the company's algorithm-supported decision making? Actions toward remediation by businesses may take various forms depending on the nature of the harm and the level of the business's involvement. Further guidance can be found in B-Tech's foundational paper on remedy in the technology sector.

© United Nations Human Rights Office of the High Commissioner

CARD 3

High-Risk Customers or End-Users

For use when a company's commercial success appears to depend on, in part or in full, its products and services being used by high-risk customers or end-users.

OVERVIEW OF THE ISSUE

Technologies may take on added risk when sold to certain categories of customers or end-users. These customers and end-users may carry additional human rights risk for various reasons. Some examples include:

Customers and end-users in law enforcement. It is not inherently problematic for technology companies to do business involving law enforcement as customers or end-users. However, the powers of law enforcement bodies within the criminal justice system, including the ability to detain people and to employ lethal force, mean that the potential harms associated with certain technologies may be heightened in law enforcement contexts. For example, when used inappropriately and/or indiscriminately, facial recognition technologies and other forms of police surveillance carry potential for use in furtherance of human rights violations, including the right to privacy as well as other rights that may be violated following unlawful arrests or detentions facilitated by these technologies.

Other examples include the sale of surveillance and data management systems to customs and immigration agencies where there is a risk of documented abuses during monitoring, arrest, detention, and deportation of immigrants, refugees, and asylum seekers.

Customers and end-users in government. Likewise, technology companies are free to do business with non-law enforcement government agencies, and many such transactions take place without posing a risk to human rights. However, due to States' wide-ranging capacity to infringe on human rights, for example by carrying out surveillance or punishing political dissent, the sale of technology products and services to State agencies can carry heightened human rights risk.

State-sponsored surveillance can constitute a substantial violation of human rights. This can include both an initial violation of the rights to privacy and free expression as well as further violations of the civil and political rights of political opposition figures, human rights defenders, and others identified by the surveillance. Technology companies have reportedly helped to sell and develop surveillance technologies[2] for central governments in States with records of these rights violations; producers of spyware products have also reportedly sold extensively to governments with poor rights records.

[2] "Surveillance technology" is a broad category, encompassing not only tools like spyware or biometric recognition products, but all products or services "that can be used to detect, monitor, intercept, collect, exploit, preserve, protect, transmit, and/or retain sensitive data, identifying information, or communications concerning individuals or groups." See https://www.state.gov/wp-content/uploads/2020/09/DRL-Industry-Guidance-Project-FINAL-508.pdf.

© United Nations Human Rights Office of the High Commissioner

High-risk private sector customers and end-users. Technology companies' sales relationships with private sector customers and end-users can also carry risk of adverse human rights impacts if those customers are connected to patterns of causing, contributing to, or being linked to human rights violations. Examples may include selling social media software solutions to customers or end-users who have reportedly used that software to track and hinder unionisation efforts.

ENGAGEMENT QUESTIONS

1. Does the board consider, as part of its decision making, risks to human rights associated with high-risk customers or end-users?
2. Does an executive oversee processes to review potential sales/licensing of, or access to, its technologies by private and public sector actors for which misuse or abuse is high?
3. Does the company take steps to mitigate human rights risks that flow, at least in part, from the goals, activities, or track records of private and public sector customers/end-users? Examples of action could include internal controls and escalations, regular testing/modifying of its technologies, contractual safeguards, technological safeguards, ongoing monitoring of end-use, and capacity building for customers or end-users.
4. Does the company collaborate with relevant stakeholders, peer companies and/or experts to mitigate systemic risks to human rights associated with high-risk customers or users?
5. Does the company take preemptive steps to increase access to remedy for individuals that are exposed to the most severe human rights risks associated with high-risk customers or users? Actions toward remediation by businesses may take various forms depending on the nature of the harm and the level of the business's involvement. Further guidance can be found in B-Tech's foundational paper on remedy in the technology sector.

© United Nations Human Rights Office of the High Commissioner

CARD 4

Conflict-Affected and High-Risk Areas

For use when a company's commercial success appears to depend on, in part or in full, its products and services being used in conflict-affected and high-risk areas.

OVERVIEW OF THE ISSUE

The lethal nature of armed conflict and other forms of widespread violence means that the risk of gross human rights abuses is heightened in conflict-affected areas. Among these risks is that technology sector products or services sold into conflict-affected and high-risk areas (CAHRAs) have the potential to be used to facilitate violations of international humanitarian law (IHL) as well as international human rights law (IHRL).[3]

These risks can unfold in various ways. Some technology companies create products or services that have direct applications in the context of armed conflict. Examples include private development of software systems for use by national militaries, efforts to develop artificial intelligence-based tools and systems for use in armed conflict, including in military drone surveillance, or the sale of technologically advanced tactical gear to military customers. It is not the case that the development and sale of such products and services necessarily carry an unacceptable level of human rights risk—this will depend on a number of factors, including whether the intended customer or end-user has a demonstrated history of IHL and/or IHRL violations. However, these technologies do carry heightened human rights risk relative to those without applications in armed conflict, and thus require a heightened level of human rights due diligence from companies.

There is also heightened human rights risk associated with the sale of "dual-use goods" (those with both civilian and military capabilities) to customers who operate or do business in CAHRAs. Examples include sales to such customers of consumer technologies that also have surveillance applications or dual-use computer chips used in weapons systems.

There are also human rights risks for technology companies to consider when doing business in CAHRAs, even when the company's products or services do not have military applications. Social media companies, for example, may confront considerable human rights risks when their products and services are used in CAHRAs; in such contexts, the spread of misinformation and disinformation can have deadly results, and social media platforms are at risk of being used to incite violence.

Finally, risks associated with doing business in CAHRAs often intersect with the surveillance and censorship-related risks discussed in Card 3. One example is the response of telecommunications companies when called upon by governments to limit or restrict access to the internet during times of political unrest; international human rights

[3] According to the Organization for Economic Cooperation and Development (OECD), Conflict-affected and high-risk areas (CAHRAs) are "identified by the presence of armed conflict, widespread violence or other risks of harm to people. … High-risk areas may include areas of political instability or repression, institutional weakness, insecurity, collapse of civil infrastructure and widespread violence." See https://www.oecd.org/corporate/mne/GuidanceEdition2.pdf

© United Nations Human Rights Office of the High Commissioner

experts have described such "internet kill switches" as violations of international human rights law. Another example is the potential for technology sector products or services to be used in the building and implementation of surveillance and censorship states in contexts of political instability or repression.

Sales of some technology products and services associated with this business model feature may be governed by existing law or guidance pertaining to the international transfer of weapons[4] or surveillance technologies.[5] In all cases, however, technology companies have a responsibility to respect human rights under the UNGPs, including robust human rights due diligence processes, above and beyond compliance with export control laws. Moreover, as the UN Working Group on Business and Human Rights points out, in CAHRAs, due diligence by business should be heightened accordingly, and should include a robust conflict analysis in order to understand the scope of potential human rights risks.

ENGAGEMENT QUESTIONS

1. Does the board consider, as part of its decision making, risks to human rights and risk of involvement in violations of IHL and IHRL associated with the use of its technologies in conflict-affected and high-risk areas (CAHRAs)?
2. Does an executive oversee processes to review the sale or use of its technologies in CAHRAs to identify human rights and IHL risks?
3. Does the company take steps to mitigate human rights and IHL risks associated with use of its technologies in CAHRAs? Examples of action could include conflict and human rights impact assessments, internal controls and escalations, regular testing/modifying of its technologies, technological safeguards, contractual safeguards, ongoing monitoring of end-use, or capacity building for customers or end-users.
4. Does the company collaborate with relevant stakeholders, peer companies and/or experts to mitigate systemic risks to human rights or risks of involvement in IHL violations associated with use of its technologies in CAHRAs?
5. Does the company take preemptive steps to increase access to remedy for individuals that are exposed to the most severe human rights and IHL risks associated with use of its technologies in CAHRAs? Actions toward remediation by businesses may take various forms depending on the nature of the harm and the level of the business's involvement. Further guidance can be found in B-Tech's foundational paper on remedy in the technology sector.

[4] For example, see https://www.thearmstradetreaty.org/hyper-images/file/TheArmsTradeTreaty1/TheArmsTradeTreaty.pdf

[5] For example, see https://www.federalregister.gov/documents/2021/10/21/2021-22774/information-security-controls-cybersecurity-items

© United Nations Human Rights Office of the High Commissioner

CARD 5

Low Leverage Sales Practices

For use when a company's commercial success appears to depend on, in part or in full, sales practices, relationships or models that limit the company's ability to observe and act upon human rights risks associated with the use of its products or services. This may include (1) sales practices that afford the company, as a matter of standard practice or law, limited leverage over the way in which end-users utilise its products or services and (2) sales practices that afford the company limited visibility into who its end-users are.

OVERVIEW OF THE ISSUE

The channels through which technology companies sell their products and services to customers or end-users can carry their own sets of human rights risks, depending on the structures of sales models and practices themselves. The UNGPs call on businesses to use their leverage—which exists "where [an] enterprise has the ability to effect change in the wrongful practices of an entity that causes a harm"—to mitigate adverse human rights impacts to the greatest extent possible. Where sales practices prevent businesses from obtaining or exercising that leverage vis-à-vis end-users, risks of human rights harms are elevated.

One example of a sales practice that can limit company leverage and elevate human rights risk is chain selling, wherein technology companies' products and services reach their ultimate customers and end-users via a long chain composed of numerous sales partners. When technology companies sell their products or services through partner resellers, downstream resellers may bundle the original company's offering with those from other vendors. This hinders companies' ability to observe how their products or services may ultimately be involved in misuse and can leave them with limited leverage to influence how and for what purposes end-users utilise their products.

A lack of visibility into who exactly a company's customers or end-users are can also enhance human rights risk. For example, "low-touch" sales models—which are sometimes used in the cloud computing sector—can grant technology companies limited visibility of who their customers and end-users are prior to a sale, and thus of how their products or services are ultimately used. Models with the lowest levels of visibility, in which customers never interact with a human in the course of buying products or services, are sometimes called "touchless conversion" sales models.

This kind of sales model can prevent companies from fully understanding how customers are using (or abusing or misusing) their products and can preclude the use of effective customer gating measures. Despite these risks, some technology companies continue to utilise sales models that limit visibility of customers or end-users, and a recent academic journal article raises concerns about the extent of due diligence done by the industry leaders in this area.

© United Nations Human Rights Office of the High Commissioner

Human rights risks may also arise where there is a disparity in status or contractual mechanisms between a technology company and a customer or end-user. For example, if a technology company enters a sales agreement with a State body that contracts on non-negotiable terms based on national security justifications, this may limit the company's leverage over the end-use of its products. In such cases, any conditions on business put in place by States do not absolve technology companies of their responsibilities to respect human rights under the UNGPs.

ENGAGEMENT QUESTIONS

1. Does the board consider, as part of its decision making, risks to human rights associated with the use of the company's technologies by customers or end-users with whom the company, as a matter of standard practice or law, has limited leverage?
2. Does an executive oversee processes to assess human rights risks associated with the use of its technologies by customers or end-users with whom the company has limited leverage? Depending on the company and its business model, situations of relevance can include:
   - The company uses distributors and resellers to get its product to market
   - The company's products or services are purchased via online or automated portals.
   - State customers invoke national security or other laws that have the effect of restraining use of leverage and transparency by the company
3. Does the company take steps to mitigate human rights risks associated with the use of its technologies by customers or end-users with which the company has limited leverage? Examples of action could include internal controls and escalations, regular testing/modifying of its technologies, technological safeguards, contractual safeguards, communicating clearly with customers and sales partners about prohibited and unsupported uses of the company's products and services or human rights-related capacity building for its internal sales teams, customers, end-users, distributors, and resellers.
4. Does the company collaborate with relevant stakeholders, peer companies and/or experts to mitigate risks to human rights associated with use of its technologies by customers or end-users with which the company has limited leverage?
5. Does the company take pre-emptive steps to increase access to remedy for individuals that are exposed to the most severe human rights risks associated with use of its technologies by customers or end-user with which the company has limited leverage? Actions toward remediation by businesses may take various forms depending on the nature of the harm and the level of the business's involvement. Further guidance can be found in B-Tech's foundational paper on remedy in the technology sector.

© United Nations Human Rights Office of the High Commissioner

B-Tech

OHCHR-b-techproject@un.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

© United Nations Human Rights Office of the High Commissioner