



**INVESTOR ALLIANCE
FOR HUMAN RIGHTS**
AN INITIATIVE OF ICCR

SECTOR-WIDE RISK ASSESSMENT: Information and Communications Technology (ICT)

SALIENT ISSUE BRIEFING: Child Rights

CONTENTS

- | | | | |
|---|---|----|--|
| 2 | Summary | 8 | Human Rights
Guidance for Business
on Child Rights |
| 3 | International Standards | | |
| 5 | How do ICT Companies
Adversely Impact Child
Rights in Practice? | 11 | Investor Guidance
on Engaging ICT
Companies |
| 7 | The 'Business Case' for
Respecting Child Rights
in the ICT Sector | 13 | Investor Efforts |



**INVESTOR ALLIANCE
FOR HUMAN RIGHTS**
AN INITIATIVE OF ICCR

SECTOR-WIDE RISK ASSESSMENT:

Information and Communications Technology (ICT)

SALIENT ISSUE BRIEFING:

Child Rights

Child rights are a salient human rights issue in the Information and Communication Technologies (ICT) sector. The concept of ‘salience’ focuses on risk to people, not to the company while recognizing that where risks to human rights are greatest, there is significant convergence with business risk. Salient human rights issues stand out because they are at risk of the most severe negative impacts through companies’ activities and business relationships. The UN Guiding Principles on Business and Human Rights (UNGPs) elaborate that companies should prioritize addressing those impacts that are most severe or where delayed response would make them irremediable.

There have been many advances in ICT and the sector continues to have the potential to improve the lives of children in several ways, including providing greater access to education, healthcare, and other public services, facilitating social connectivity, and helping child service providers deliver resources more efficiently. When applied responsibly, ICT can expand children’s opportunities and support their enjoyment of rights.

Yet, ICT also exposes children to higher risks both in the digital and physical world. Through online platforms, online gaming communities, and messaging applications, there has been an exponential increase in online predators targeting children, particularly during the coronavirus pandemic. The digital marketing ecosystem also has adverse impacts on children’s rights – from breaches of privacy to the marketing of harmful products. Artificial Intelligence is shaping children’s emotional development in confusing ways, and children already experiencing unequal access to digital resources are at risk of falling further behind their peers. These risks to children are rapidly evolving, leading to wide-ranging potential and actual negative impacts.

Under increased public scrutiny, the ICT sector has begun to address these challenges, albeit not yet sufficiently. Generally considered to be a good investment in terms of ESG and financial performance, ICT companies are increasingly coming under pressure from investors who are engaging with these companies on their human rights performance in a robust and organized fashion. ICT companies have a responsibility to address their impacts on child rights to ensure they are not causing, contributing, or directly linked to harm.



INTERNATIONAL STANDARDS¹

According to Article 25 of the [Universal Declaration of Human Rights](#) (UDHR), children are entitled to “special care and assistance.” In addition, Article 3 of the [Convention on the Rights of the Child](#) (CRC) specifies that “In all actions concerning children...the best interests of the child shall be a primary consideration.” Both treaties emphasize that childhood is a vulnerable period of time in a human’s life, necessitating unique rights and additional protections. Companies have a responsibility to adhere to these standards when integrating technology into the lives of children and in doing so, should consider their evolving capacities given that the “risks and opportunities associated with children’s engagement in the digital environment change depending on their age and stage of development” ([UNCRC General Comment No. 25](#)).

The CRC offers the most detailed outline of rights belonging to every child, defined as “every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier” (Article 1). The principle of non-discrimination covers these rights, guaranteeing the enjoyment of rights to all children with no distinction on the basis of “race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status” (CRC Article 2) or “reasons of parentage,” ([International Convention on Economic, Social and Cultural Rights](#) Article 10). The CRC also provides that children have “inherent dignity and...equal and inalienable rights” as any human being. Notwithstanding their vulnerability and recognizing the importance of enabling children to develop and exercise their own agency, the CRC provides children the right to freely express their views and opinions (Article 13), notably in matters that affect them (Article 12), and the right to have “access to information and material from a diversity of national and international sources” (Article 17). Similar to the UDHR, these rights coexist with protections such as the right to privacy (UDHR Article 12 and CRC Article 16); however, the CRC includes additional specific obligations such as ensuring the child’s protection from harmful media content (Article 17) and any forms of violence, neglect, or exploitation (Article 19) and sexual abuse (Article 34).

In March 2021, the [UN Committee on the Rights of the Child](#) declared that “the rights of every child must be respected, protected and fulfilled in the digital environment.” Through consultation, the Committee heard from children who stated that they “would like the government, technology companies and teachers to help [them] to manage untrustworthy information online [and] would like to obtain clarity about what really happens with [their] data.” The Committee called on the business sector, which impacts children’s rights “directly and indirectly in the provision of services and products relating to the digital environment... [to] respect children’s rights and prevent and remedy abuse of their rights in relation to the digital environment.”

Children rely on the internet to receive their education and exercise their social and cultural rights. To address the negative consequence of this dependency, particularly, “the growing availability of [child sexual abuse materials] on the Internet and other evolving technologies,” the [Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution, and child pornography](#) asks States to take measures to protect the rights of child victims, their privacy, and their safety (Article 8). Building on the special rights accorded to children in the UDHR and CRC, in the European Union, the [General Data Protection Regulation](#) expressly affirms that “Children merit specific protection with regard to their personal data” (GDPR Recital 38) and sets an age limit of at least 16 years old on the “processing of the personal data of a child,” although States may choose to set the age at 13 or above (GDPR Article 8).

Safeguarding the rights of children is a collaborative process involving several stakeholders including parents, caregivers, governments, public and private institutions, civil society organizations, courts of law, administrative authorities, and legislative bodies. As the lives of children increasingly extend to the digital environment, so do the responsibilities of stakeholders to respect and protect the rights of children.

¹ For this briefing, we refer to international standards that focus on the impact technology has on child rights at the end-use of products and services and do not address risks in technology manufacturing supply chains.

RESOURCES

Guidance:

- The UK Information Commissioner Office's [Age Appropriate Design: A Code of Practice for Online Services](#) details the data protection safeguards that should guide the provision of online services to ensure they are appropriate in meeting the developmental needs of children in line with the GDPR.
- Save the Children created a guide on [Child-Centered Design](#) that integrates three nodes: children's rights, positive recognition, and service design. The guide details the process of working with children and steps to integrate their input into developing better services.
- Australia, Canada, New Zealand, the U.K., and the U.S. in consultation with six leading platforms (Facebook, Google, Microsoft, Roblox, Snap, Twitter) developed a framework to support existing industry efforts called [Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse](#). [WeProtect Global Alliance](#) has developed a guide for tech companies considering supporting the Voluntary Principles.
- The [Australian Safety by Design Principles](#), developed by Australia's eSafety Commissioner's office in consultation with young people, aims to provide online and digital interactive services with a clear and broadly applicable set of guidelines for the better protection of users.
- The United Nations Office of the High Commissioner for Human Rights B-Tech Project provides guidance and resources to support technology companies in implementing the UNGPs, including foundational papers on [Identifying Human Risks Related to End-Use](#) and [Taking Action to Address Human Rights Risks Related to End-Use](#).
- [for the Online Gaming Industry on Assessing Impact on Children \(2020\)](#). UNICEF has also produced a series of [discussion papers](#) unpacking key issues related to children's rights and business in the digital environment. These resources complement the [2020 Guidelines for Industry on Child Online Protection](#) developed by the International Telecommunications Union (ITU) and partners.
- An NGO, [Thorn](#), builds technological tools to combat the spread of child sexual abuse material (CSAM). Thorn's technology called [Safer](#) allows companies hosting user-generated content to identify, remove, and report CSAM at scale.
- The [Global Campus for Human Rights](#) offers a course on children's rights in the digital age. The course has five modules that provide an overview of the various impacts of technology on child rights.

Multi-Stakeholder Initiatives:

- [WeProtect Global Alliance](#) comprises governments, companies, civil society organizations, and international organizations working together to strengthen the global response to online child sexual exploitation and abuse.
 - The [Tech Coalition](#) is a global alliance of leading technology firms that work to develop tools and programs that protect children from online sexual exploitation and abuse.
 - The [Global Child Forum](#) is a collaborative platform that brings together businesses, civil society groups, academia, and governments to promote children's rights. The organization focuses on the role of businesses in driving social change and benchmarks companies' respect for child rights, including a recently published [deep-dive benchmark](#) of 252 ICT companies.
- The UN Children's Fund, UNICEF, developed a set of [tools for ICT companies](#) on supporting child rights due diligence processes, including a 2021 edition of the child rights impact self-assessment tool for mobile operators ([MO-CRIA](#)) and [Recommendations](#)

Online Tools & Courses:



HOW DO ICT COMPANIES ADVERSELY IMPACT CHILD RIGHTS IN PRACTICE?

Children as rights holders are unique in that business activity that may not have adverse impacts on adults may negatively affect their rights. The following table outlines several ways that ICT companies can adversely impact children's rights based on the [OECD's typology of risks to children in the digital environment](#):

Risk Categories	Examples of Risk Manifestations
Content Risk	Failing to apply appropriate content moderation and age restrictions to prevent access to harmful and illegal online content (e.g. <u>loopholes in Apple's policies allow children to download apps showcasing sexual content</u> ; <u>Tik Tok's algorithm serves sex and drug videos to minors</u>).
Conduct Risk	Poorly enforcing ethical standards and codes of conduct that caution against using products and services to carry out hateful and problematic behavior (e.g. <u>Snapchat's disappearing message feature shaping cyberbullying tactics</u> ; <u>students creating anonymous social media accounts to instigate bullying and harassment</u>).
Contact Risk	Enabling perpetrators access to advanced technologies and platforms they can use to groom children online, commit sexual abuse, and <u>accelerate the spread of CSAM online</u> (e.g. <u>sexual predators posing as children in video game chat rooms</u> ; <u>CSAM rampant on platforms offering anonymous Internet access</u> ; <u>at least half of online grooming offenses in the UK took place on Facebook-owned apps</u>).
Consumer Risk	Using targeted advertising to exploit children's preferences and limited comprehension skills (e.g. <u>advertising e-cigarettes as confectionery flavors</u> ; <u>ads for junk food disproportionately target Black and Hispanic children in the U.S.</u>).

Cross-Cutting Risk

Collecting vast amounts of children's data and selling them without permission (e.g. study finds Facebook and Instagram are gathering browsing history of users under 18; TikTok accused of sending users' biometric data overseas).

Facilitating surveillance and tracking of children from vulnerable, historically marginalized, or underrepresented groups (e.g. E.U. deploys biometric technology to track refugee and migrant children; increase in the collection of migrant children's fingerprints by U.S. Customs and Border Patrol).

Reinforcing systemic bias and discrimination by applying flawed data to predictive analytics (e.g. frequent exposure to algorithmic discrimination can negatively impact teens' self-image and mental health; New York City weighs the negative implications of using predictive analytics for child welfare services).

Widening the digital divide between children from vulnerable social groups, especially young girls, and their peers. Lack of access to the internet and emerging technologies, such as AI-enabled services, exacerbate social inequalities. Children that do not interact with AI tools risk being left behind in a world increasingly powered by AI (e.g. limited access to the internet negatively impacting educational outcomes of children around the world).

Data protection concerns specific to children

Existing privacy and fairness concerns stemming from the collection of adults' data are magnified when it comes to the collection of data from children, given their greater cognitive, emotional, and physical vulnerabilities. The implications of surveillance and tracking are also more significant for children due to greater exposure over their lifetime, and due to the importance of childhood as a time for development and experimentation with identity. How data is collected, stored, and processed affects how data is then used to inform decisions that affect children's current and future lives.

It is vital that technology companies providing services that may be accessed by children ensure they have staff trained on child rights as well as a focal point for children's data governance. This focal point must be accessible by children and their representatives who wish to make subject access requests or seek clarification about other aspects of the use

and management of their data by the company. Large teams of staff trained in children's data rights may be required where companies have an extensive regional or global reach.

Technology companies should adhere to [data minimization principles](#), meaning that when they do collect data, it should be the minimum amount strictly necessary to perform the functions they provide. By limiting the data they collect, companies can reduce the potential and real harms perpetuated using people's personal information. As explained by the [UNICEF Manifesto on Good Data Governance for Children](#), children are more vulnerable than adults and are even less able to understand the long-term implications of consenting to their data collection. While data on individuals tend to be treated the same way regardless of who the individual is, children's data deserve to be treated differently.

How does Artificial Intelligence impact children's rights?

The rapid deployment of Artificial Intelligence (AI) into the activities of daily life, facilitated using data-driven machine learning, has the greatest impact on children. AI will determine their access to healthcare, education, and future work opportunities as impacted by automation. ICT companies must recognize that as facilitators of these changes, they have a responsibility to prevent and mitigate the adverse impacts their innovation has on children.

Although providing the opportunity to improve children's lives, AI also carries with it tremendous risks, including a lack of protection practices to minimize data collection (see "Data Protection Concerns Specific to Children"). AI systems often rely on data that is personal, and since children are less aware of the consequences of providing such data they may be inclined to share too much of their information.

In other cases, children may interact with AI systems that were not designed for them, or individuals may use AI in ways that affect children directly or indirectly. When chatbots designed to support mental health by simulating human-

like conversations fail to recognize appeals from children, they [risk augmenting their distress](#) since children may not have the emotional resilience to deal with a dismissive or puzzling response. Other studies have shown that because their cognitive skills are not yet fully developed, younger children are more likely to [anthropomorphize social robots](#). When AI systems become children's method of socialization, it affects their understanding of reality, shapes their social environment, and molds their thinking and personalities.

[UNICEF](#) provides three foundations to guide AI policies and systems to better align with children's rights and needs: *protection, provision, and participation*. **Protection** invokes the "do no harm" principle, meaning ICT companies should design AI in the safest way for children. **Provision** means that AI should "do good" so that all children benefit from the opportunities AI provides. Lastly, through **participation**, children should have the agency to shape AI and AI should in exchange improve their agency. Designing AI systems and policies on these three foundations is a start to ensuring AI serves the positive development of children.

The dilemma of identifying and removing CSAM without violating privacy rights

Balancing the right to privacy with the urgent response needed to combat online child sexual exploitation and abuse (OCSEA) is an increasing debate amongst experts. In 2020, the National Center for Missing and Exploited Children (NCMEC) received 21.7 million reports of online exploitation of children that included 65.4 million images, videos, and other files containing child sexual abuse material (CSAM). However, policies to address online exploitation of children and production of CSAM can conflict with the right to privacy, including children's. In order to identify and remove CSAM, ICT companies may implement mechanisms that undermine privacy and security, or conversely, implement privacy protocols that make detecting child sexual abuse difficult.

Apple is a recent example of a company caught at the crossroads of this dilemma. In August 2021, the company announced child protection measures that included a device scanning feature that would scan all the photos uploaded to iCloud, as well as monitoring certain images sent via iMessage, for CSAM. However, privacy experts argued that implementing the device scanning features could be used as a tool to normalize surveillance, undermine encryption, and introduce vulnerabilities in the system. In response to various feedback, Apple delayed the rollout of the scanning technology and took steps to review and make improvements.

In contrast to Apple, Facebook announced privacy-focused policies in 2019 that made it more difficult for law enforcement and the company to detect CSAM on its platforms. This move was concerning considering that Facebook and its other platforms (Messenger, Instagram, and WhatsApp) accounted for 94 percent of online child sexual abuse cases reported to NCMEC by electronic service providers.

Encryption is at the center of the dilemma between child protection and privacy. In INTERPOL's resolution calling for increased safeguards against online child sexual exploitation, the General Assembly noted the challenges end-to-end encryption posed to law enforcement as it is used to "conceal illicit online crimes against children such as grooming, live streaming of sexual abuse and the distribution of child sexual abuse material." Yet, encryption is important for protecting human rights and ensuring children's safety online. It safeguards the freedom of expression and privacy of individuals in countries where people face persecution for commenting on political or social issues, and ensures that digital devices and communications containing personal information that could compromise children's safety remain secure and private.

Several governments are beginning to tackle this dilemma as well. The European Union is working towards strategies for detecting crimes, such as online CSAM, while maintaining the privacy protections encrypted communications provide. The Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse, initiated by five governments, takes into account privacy considerations. The Committee on the Rights of the Child in General Comment No. 25 advises that where encryption is necessary, "appropriate measures enabling the detection and reporting of child sexual exploitation and abuse or child sexual abuse material...must be strictly limited according to the principles of legality, necessity, and proportionality." Achieving this balance around the globe on all online platforms will require innovative solutions from ICT companies, regulation and coordination among governments and international organizations, and engagement with civil society organizations and other key stakeholders.



THE 'BUSINESS CASE' FOR RESPECTING CHILD RIGHTS IN THE ICT SECTOR

Respecting child rights is a matter of sustainability given that children account for one-third of the world's population and represent the future of our society. Designing with children in mind also offers businesses opportunities to grow and

expand their target market. Partnerships between technology companies and schools to improve student access to education are part of government strategies and budgets, potentially introducing businesses to new streams of capital.

Providing technology that helps children in remote areas of the world learn can open new markets for companies. In contrast to opportunities to grow, harmful business practices can pose material risks for companies.

ICT companies need to engage with young people as well as child rights advocates and experts as stakeholders or potentially face reputational consequences. While children use technology for connectivity, learning, and socialization, they also use it strategically as a tool to organize. The rapid rate at which young people adopt ICT enhances their civic engagement and access to tools for activism. Online platforms, particularly social media, have mobilized young people around the world to engage in social justice issues, from racism to climate change and gun violence. The global youth-led climate protests in 2019, which attracted tech workers from Amazon and Google, were proof that young people are attentive to issues affecting their lives. Their concern extends to privacy matters. In 2020, students protested against the use of Proctorio, a digital monitoring software, which they argued was invasive and perpetuated harmful biases. When designing products and services, companies must integrate child-rights-centered design or risk facing such consumer backlash.

Failure to respect child rights subjects companies to serious reputational and legal risks, and a business risk is a risk to investors. To hold tech companies responsible for the proliferation of CSAM on their platforms, U.S. lawmakers have introduced the Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2022 and, in Europe, officials are demanding a shift from voluntary reports to a law requiring tech companies to combat child sexual abuse. The consequences for failing to respect child rights also carry financial risks. A complaint filed with the U.S. Federal Trade Commission accused three tech companies operating a coloring book app of collecting personal information from children without their consent, a violation of the Children’s Online Privacy Protection Act (COPPA). Under a Department of Justice settlement, the court ordered the companies to pay \$3 million dollars. Oath, a Verizon-owned company, paid \$5 million in settlement for targeting ads at children using their personal data. In another case, representatives of minors filed 21 lawsuits against TikTok for collecting and selling children’s data to third parties without permission, which resulted in a \$92 million settlement. ICT respect for child rights helps to not only prevent and mitigate risks to children but also protects business and investment value.



HUMAN RIGHTS GUIDANCE FOR BUSINESS ON CHILD RIGHTS

Drawing from the UN Guiding Principles on Business and Human Rights, the Children’s Rights and Business Principles, and the International Telecommunication Union’s Guidelines for Industry on Child Online Protection, the following guidance for businesses to prevent, mitigate, and address adverse impacts on children’s rights helps to inform investor engagement with ICT companies.

UNGPs	Implementation	Good Practice Recommendations
<p><i>Develop a policy commitment and embed respect for child rights into business</i></p>	<p>Companies should consult with civil society and stakeholders in developing a policy commitment on child rights that recognizes international human rights standards. The policy should be discussed, reviewed, and approved by senior leadership, distributed internally, and shared publicly with all users, customers, business partners and suppliers through terms of service, codes of conduct,</p>	<p>→ Companies should establish in corporate policies and technical guidance for all personnel involved in the life cycle of products and services (design, deployment, and implementation) that protecting children’s rights guides all business operations.</p>

	<p>or contracts. Furthermore, the policy's implementation should be adequately resourced and regularly reported to senior leadership.</p>	
<p>Assess actual and potential impacts on children</p>	<p>Through engagement with affected stakeholders and relevant experts, companies should identify and assess real and potential adverse impacts that business operations and technological products and services in their value chain have on children. The focus should be on salient risks to children, particularly vulnerable and marginalized children, and not solely to the company. Companies should draw on external expertise when engaging with children to ensure child-sensitive engagement practices.</p>	<ul style="list-style-type: none"> → Child rights impact assessments should be an ongoing process, conducted for new markets, business relationships, and technological applications, e.g. facial recognition or algorithmic machine learning and decision-making technologies, as well as when there are changes in the operating environment. → In-depth, stand-alone assessments may be needed for severe actual and potential impacts – for example, risks of child sexual exploitation online, AI systems that reinforce discrimination, exposure to age-inappropriate content, and violations of privacy.
<p>Integrate child rights considerations into broader company policies and activities based on findings of assessments</p>	<p>Drawing on their child rights impact assessments, companies should integrate the assessment findings across relevant internal functions and processes (with clear assignment of roles, responsibilities, and resources and senior-level oversight). Where a company is causing or contributing to real or potential adverse impacts on children's rights, it should take steps to promptly cease or prevent the activity and use its leverage to mitigate the impact. Where companies are directly linked to adverse impacts through business relationships, they should seek to increase and utilize their leverage to address them.</p>	<ul style="list-style-type: none"> → Implement minimum age requirements and support research and development of robust and rights-respecting age assurance tools. → Those hosting user-generated content and advancing user connection should collaborate with government, law enforcement, civil society, and hotline organizations to develop standard processes on addressing CSAM. → Increase leverage by acting collectively. For example, companies may choose to join multistakeholder initiatives such as the Tech Coalition, an alliance platform for tech companies working to address online child sexual exploitation and abuse. → Take steps to increase accessibility of products and services while ensuring they are suitable for children to use, particularly for children with disabilities. → Adopt proactive <u>child safeguarding measures</u> to ensure that direct or indirect contact with the company (i.e. through employees, business partners, etc.) does not result in harm. For example, offer targeted training to personnel and business partners to require respect for children's rights across business operations.

<p>Monitor performance</p>	<p>Companies should track their responses to adverse impacts in order to verify they are being addressed effectively. Companies should use appropriate qualitative and quantitative indicators and draw on feedback from internal and external sources, including affected children, families, and other stakeholders in tracking performance.</p>	<ul style="list-style-type: none"> → Document company practice for handling CSAM from when the content is detected, to its removal, and subsequent destruction. → Monitor to ensure that AI systems using algorithms, machine learning, and automated decision-making are not having unintended negative impacts, such as discriminatory outcomes. Internal or external independent auditing of AI systems presents one option. AI code should be fully auditable and audit results should be disclosed.
<p>Communicate performance</p>	<p>Companies should communicate externally their efforts to address the business impact on children’s rights regularly. Companies should make this material accessible to their intended audiences, for example in annual human rights and sustainability reports, and provide adequate information for evaluating the company’s efforts to respond to salient risks to child rights. Formal reporting should occur where risks of severe impacts exist.</p>	<ul style="list-style-type: none"> → For users and other stakeholders to understand the impact of AI systems on child rights, companies should communicate among other things: when and how AI technologies are deployed; the logic used by those systems; policies that direct their use; which decisions in the information environment are made by automated systems and/or human review; and when the personal data of children will become part of a dataset and how it will be used.
<p>Remediate</p>	<p>When companies cause or contribute to adverse impacts on children’s rights, they should provide for or cooperate in remediation through legitimate grievance mechanisms at the operational or judicial level, as appropriate. Operational level mechanisms must be <u>accessible to children</u>, as well as their families and representatives. Outcomes of the grievance mechanism should flow into risk assessment processes.</p>	<ul style="list-style-type: none"> → Create reporting mechanisms so that affected users and their representatives can raise concerns about child rights violations (e.g. grooming, CSAM, harmful and inappropriate content, privacy breaches). → Companies should participate in state-based judicial and non-judicial grievance and remediation mechanisms.



INVESTOR GUIDANCE ON ENGAGING ICT COMPANIES

The following questions, drawn from the [Children's Rights and Business Principles](#) and [Tool for Investors on Integrating Children's Rights Into ESG Assessment](#), are intended as a starting point for investors engaging with ICT companies to help them evaluate if companies are making adequate efforts to implement their responsibility to respect child rights in their operations and business relationships.

Human rights commitment

- Has the company adopted a public-facing policy commitment to respect child rights in line with international standards, drawing on relevant child rights expertise? If yes, does the policy include commitments to children's rights apart from addressing child labor? Is the policy endorsed by the Board and CEO of the company?
- Does the company have safeguarding policies and measures to protect children using their products and services in recognition of children as unique rights holders requiring additional consideration?
- Does the commitment apply to suppliers, and other business partners throughout the company's value chain, and are they communicated as a responsibility guiding their business relationships?

Governance

- Is there a Board Committee tasked with oversight of child rights and regularly reporting these findings to the Board members? Does the Board have appropriate expertise on child rights or access to experts? Does the Board actively engage in oversight of children's rights issues and review connections between the company's operations and impacts on child rights?
- Are the company's lobbying and political contributions in line with commitments to protect children's rights?
- Are respect for children's rights incorporated into the company's business strategy and processes?

Assessing impacts, risks, and opportunities

- Does the company conduct a children's rights risk assessment, either as a stand-alone or [integrated assessment](#), of all its operations? Has the company

identified and assessed the most salient risks to children's rights? Does the company report externally on its most salient children's rights impacts and how often does the company publish this report? Has the company shared learnings from any risk and impact assessments on child rights in industry forums?

- Does the company include children and child rights advocates as a stakeholder group and consult with stakeholders in the assessment of children's rights? How frequently does the company have consultations with child rights experts? How are their inputs integrated into business activities?

Responding to risks and impacts

- Has the company developed steps to prevent and mitigate adverse impacts on children's rights and how does it evaluate the effectiveness of its efforts?
- Does the company participate in multi-stakeholder engagements with industry peers, NGOs, civil society organizations, and governments that support advancing children's rights?
- How does the company use its leverage in business relationships to reduce adverse impacts on child rights?
- Does the company have policies on integrating child-centered design into developing its products and services, including AI-powered tools? How does the company ensure AI systems are not reinforcing bias and causing unintended harm to children?

Embedding commitments internally and externally

- How will the company disseminate children's rights commitments to internal and external stakeholders and throughout its value chain? How does the company audit or monitor to ensure its partners, suppliers, and

other key relationships are following the company's policies? Does the company offer training to personnel and business partners on its children's rights commitments?

- Does the company publicly communicate in its policies respect for children's rights to users of its technologies, services, and products? How does it address cases of users violating terms of services, such as violating children's privacy, spreading child sexual material online, or cyberbullying?

Ensuring access to remedy

- Does the company provide or participate in timely, accessible, and effective grievance mechanisms to offer children and/or their representatives access to remedy when their rights have been harmed?
- Does the company periodically assess and disclose information about the effectiveness of grievance mechanisms? Does the company proactively notify users when they believe harm has occurred?



INVESTOR EFFORTS

Investors are taking steps to prevent and mitigate adverse impacts on children’s rights by holding ICT companies accountable. Here are some examples:

- In the 2020 proxy season, investors filed proposals urging internet service providers Verizon and AT&T and three of the largest information technology companies, Apple, Facebook, and Google, to assess “the potential sexual exploitation of children across...[their] businesses” and increase efforts to protect children from sexual exploitation online. Since then, AT&T and Verizon have conducted child rights risk and impact assessments.
- From 2020-2022, investors filed shareholder resolutions asking Facebook to report on “the risk of increased sexual exploitation of children as the Company develops and offers additional privacy tools such as end-to-end encryption.”
- In the 2020 proxy season, B.C. General Employees’ Union (BCGEU) filed a proposal asking Thomson Reuters to produce a human rights risk assessment concerning the use of its software to facilitate inhumane family separation and indefinite family detention policies at the US-Mexico border, which infringe on the rights of children to be free from arbitrary or unlawful interference with their family.
- As You Sow Foundation filed a resolution in December 2020 requesting Facebook’s Board of Directors to address several negative impacts the platform is having on human rights, including the more than 45 million CSAM made publicly available through the platform.
- Jana Partners in collaboration with the California State Teachers Retirement System (CalSTRS) engaged with Apple in 2018 to address the addictive and time-consuming intent behind its product design. In a letter made public, the two partners called on Apple “to offer parents more choices and tools to help them ensure that young consumers are using [Apple] products in an optimal manner.”
- Sustainalytics in partnership with UNICEF develops guidelines and toolkits for investors on assessing children’s rights in their investment decisions. Their most recent release, Integrating Children’s Rights Into ESG Assessment tool, builds on their existing work with UNICEF and aims to help investors understand the impact companies have on child’s rights.



**INVESTOR ALLIANCE
FOR HUMAN RIGHTS**
AN INITIATIVE OF ICCR

The **Investor Alliance for Human Rights** is a collective action platform for responsible investment that is grounded in respect for people’s fundamental rights. Along with civil society allies, we equip the investment community with expertise and opportunities to put the investor responsibility to respect human rights into practice. We do this by: (1) providing tools and resources for investor action on human rights, (2) supporting direct engagement with portfolio companies on their own human rights practices, and (3) coordinating advocacy that asks policy-makers and standard-setting bodies to create level-playing fields for responsible business. Our members are based across 20 countries and represent over \$10 trillion in assets under management and advisement. Our diverse membership includes asset managers, public and private pension funds, trade union funds, faith-based organizations, foundations, and family funds. The Alliance is an initiative of ICCR. Visit our website at: <https://investorsforhumanrights.org> and follow us on Twitter: [@InvestForRights](https://twitter.com/InvestForRights)

Developed by the Investor Alliance for Human Rights with Juliet Ihediohanma as the principal author. We would like to thank Access Now, CBIS, and UNICEF for their input on this briefing.