

10 Human Rights Priorities for the Information and Communications Technology Sector

A primer on the most relevant, urgent, and probable human rights impacts for the ICT sector and opportunities for positive impact



In 2011, the UN Human Rights Council unanimously endorsed the UN Guiding Principles on Business and Human Rights, the first international instrument to assign companies the responsibility to respect human rights.

Human rights are inherent to all human beings. They are defined and established in more than 80 international legal instruments¹ and include fundamental protections of human dignity, needs, and freedoms, such as food, housing, privacy, personal security, and democratic participation.

Since the adoption of the Universal Declaration of Human Rights (UDHR) in 1948, the duty to protect human rights has primarily fallen on governments. However, over the following decades, it became increasingly clear that the freedoms enshrined in the human rights framework could also be violated—and promoted—by the private sector.

In 2011, the UN Human Rights Council unanimously endorsed the **UN Guiding Principles on Business and Human Rights** (Guiding Principles), the first international instrument to assign companies the responsibility to respect human rights. The Guiding Principles state that governments must put in place good policies, laws, and enforcement measures to prevent companies from violating rights, that companies must refrain from negatively impacting rights, and that victims of corporate abuses must have access to effective remedy. As part of this responsibility, the Guiding Principles require companies to undertake due diligence to identify and manage their negative human rights impacts.

This issue brief identifies the 10 most salient human rights risks for Information and Communications Technology (ICT) companies, as well as opportunities for positive impact. The information here is gathered from BSR's direct engagement with ICT companies, as well as our 25 years of experience helping companies in all sectors manage their human rights risks.

The ICT sector comprises a huge range of businesses and activities, such as internet, telecommunications, consumer electronics, software, network hardware, semiconductors, and media companies. While each of these sub-sectors will have its own human rights profile and challenges, this brief highlights common industry-wide challenges. When compared to other industries, the extent to which human rights impacts occur during the entire lifecycle—manufacture, use, and disposal—of the ICT industry's products, services, and technologies is notable.

¹ Including, notably, the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), the International Covenant on Economic, Social and Cultural Rights (ICESCR), and International Labor Organisation (ILO) fundamental conventions.

Top 10 Human Rights Risks for the Information and Communications Technology Sector

1 Artificial Intelligence (AI) and Big Data Analytics

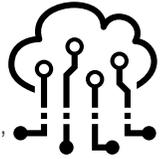
The related developments of AI and big data analytics have been enabled by more powerful computing and the ability to utilize large and complex data sets. These developments present tremendous opportunities, such as in medical diagnostics, retail, and law enforcement. However, a variety of new risks emerge with their use, such as automated systems making discriminatory decisions (such as in housing, credit, employment, and health),² the automation of jobs impacting labor rights by reducing demand for certain skills,³ or the misuse of personal data.



Reference: UDHR Articles 2, 7, 12, 23

2 Internet of Things

The networking of objects, devices, people, and organizations to create the so-called “internet of things” is enabling a wide range of new products, services, and solutions, such as smart cities, sustainable agriculture, self-driving cars, connected healthcare, and more efficient industrial processes. These opportunities are accompanied by new risks and challenges, such as the difficulty of obtaining informed consent from citizens for data use, or the need to establish privacy protocols for who has access to data, who controls data, and how data is used. These challenges form an important new social license to operate—without public trust, the internet of things is much less likely to become a commercial success.



Reference: UDHR Article 12

3 Encryption

Strong encryption (i.e. authentication of digital interactions) is increasingly accessible for everyday communications, such as email, voice, messaging, and cloud storage. Encryption provides the privacy and security necessary to exercise the right to freedom of opinion and expression in the digital age and is especially important for human rights defenders, vulnerable populations, and whistleblowers.⁴ However, law enforcement and intelligence services are concerned that encryption makes fighting crime (e.g. drugs, terrorism, and fraud) tougher, and they are using public policies or hacking techniques to prohibit and fight it. Some states are implementing or proposing “back doors” to get around encryption—but providing “special access” to government authorities can weaken everyone’s online security and privacy.



Reference: UDHR 3, 12, 18, 19

4 Hate Speech and Countering Violent Extremism

As set out in Article 19 of the UDHR, everyone has the right to freedom of opinion and expression, including the right to seek, receive, and impart information and ideas through any media and regardless of frontiers. However, governments are increasingly interested in proactive monitoring, surveilling, removing, and blocking of certain types of content, especially terrorist content and hate speech. These content restrictions are important for human rights protection but must be “necessary and proportionate” and the least intrusive restrictions to achieve the desired result.⁵ Access to appeal and remedy in the event of over-blocking is crucial.



Reference: UDHR 19, 29

5 Law Enforcement Relationships

ICT companies have relationships with law enforcement agencies, from, for example, responding to demands for user data and content restrictions or the sale of products, services, and technologies. However, companies face the risk that law enforcement agencies themselves violate human rights, such as when surveillance powers are misused, overbroad requests for data or content restrictions are made, or governments make use of hacking techniques without proper approvals.⁶ Transparency about company relationships with law enforcement agencies (including sales relationships) is increasingly important.



Reference: UDHR 3, 12, 19

6 Child Rights

As children spend more time online, it is important for companies to understand how to respect children’s rights in the digital world. This extends beyond protecting children from harmful content to include how to empower children as active digital rights holders.⁷ A comprehensive approach to child rights will incorporate children’s rights to privacy, freedom of expression, information, education, and non-discrimination and consider how to engage with children as rights holders. It will address important dilemmas, such as the role of parents, quality of available content, and need to balance child protection with important opportunities for development, discovery, learning, and expression.



Reference: UDHR 12, 19, 26; Convention on the Rights of the Child

2 https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf

3 https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf

4 https://view.officeapps.live.com/op/view.aspx?src=http%3A%2F%2Fwww.ohchr.org%2FEN%2FHRBodies%2FHRC%2FRegularSessions%2FSession29%2FDocuments%2FA.HRC.29.32_AEV.doc

5 <https://necessaryandproportionate.org/>

6 <https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf>

7 Customer Due Diligence

ICT companies can be “directly linked” to human rights impacts via the use of products, services, and technologies by their customers. While leverage to prevent negative human rights impacts during the product use phase is limited, it is important for ICT companies selling to businesses and governments to undertake customer due diligence on human rights issues, especially for public sector clients involved in law enforcement, justice, public safety, and counter terrorism activities in high risk markets. Many governments are increasingly integrating human rights factors into export controls of technologies with dual use capabilities under the Wassenaar Arrangement.⁸



Reference: UDHR Articles 1-27

8 Non-Discrimination

The underrepresentation of minorities in the ICT industry is of great concern to the whole sector. Discrimination in hiring, promotion, pay, and workplace cultural practices needs to be addressed, and solutions need to be implemented for more equal representation in the workplace. Examples of actions companies can take include robust grievance mechanisms, equal pay assessments, unconscious bias training, investment in diversifying the workforce pipeline, performance transparency, and creation of a culture of inclusion. Companies also need to be alert to different forms of discrimination—such as gender, political opinion or sexual orientation—in different countries and cultural contexts.



Reference: UDHR Articles 2, 23

9 Raw Materials Sourcing

Technology hardware relies on the sourcing of a wide range of minerals. While significant attention is paid to the “conflict minerals” of tin, tantalum, tungsten, and gold sourced from the Democratic Republic of Congo and surrounding countries, this risk is much broader. It covers other minerals (such as cobalt and copper), other locations (such as Indonesia, Ghana, and China), and a wide range of human rights issues (such as child labor, health and safety, and working hours) in addition to these specific issues of conflict. The ICT industry should focus on approaches most likely to address the root causes of these problems.



Reference: UDHR Articles 3, 4, 23, 24, 25

10 Forced and Bonded Labor

In recent years, it has become clear that the manufacture and distribution of technology hardware can involve forms of bonded and forced labor—for example, where fees are charged to workers during their recruitment or where passports and other forms of identification are withheld. In these cases it is important that recruitment fees are repaid in full to the employee and the companies end relationships with violating employment agencies if they do not demonstrate improvement.



Reference: UDHR Article 4

Top 3 Opportunities for Positive Impact

1 Human Rights by Design

A variety of disruptive products, services, and technologies (such as AI, big data analytics, and blockchain) are shaping our future. On the one hand, we have a once-in-a-generation chance to harness massive advances in technology for the public good; on the other hand, we risk unleashing into the world new technologies, capabilities, and business models that might cause significant harm. A “human rights by design” approach would build on existing “privacy by design” methodologies to ensure that other human rights issues—such as freedom of expression, non-discrimination, and child rights—are built in from the start.⁹

2 Access to Products and Services

ICT can substantially increase the access that rights holders have to a wide range of resources—such as information, healthcare, education, and financial services—that are essential to the realization of human rights. ICT can be deployed to increase public sector accountability and transparency, such as improving the fairness of elections and the responsiveness of the justice system. ICT can also unlock significant social, economic, cultural, and civil rights opportunities for women.

3 Human Rights Solutions

Collectively, the human rights community makes significant efforts to address widespread and intractable human rights violations, such as human trafficking, child exploitation, and conflict minerals. Innovative ICT technologies (such as PhotoDNA, blockchain, and big data analytics) can be deployed by governments, companies, and human rights organizations to address these challenges in new ways. ICT companies can also provide specialist advice and solutions to human rights defenders, such as in the areas of data security and privacy.

8 <http://www.wassenaar.org/>

9 <https://www.bsr.org/en/our-insights/blog-view/human-rights-by-design>

BSR's Work

Our Human Rights Expertise

We draw on a team of nearly 20 human rights experts and a network of partners from business and civil society to tackle global challenges and ensure that companies in all sectors meet and exceed global human rights standards. Our work includes surveying and benchmarking human rights practices and policies across industries to aid our member companies' efforts to craft comprehensive, responsible approaches to human rights.

 See more: <https://www.bsr.org/human-rights>

Human Rights Working Group

BSR's Human Rights Working Group brings companies together to share best practices, develop solutions, and work toward the implementation of the UN Guiding Principles.

Contact



Margaret Jungk
Managing Director, Human Rights
mjungk@bsr.org

Our Work with the ICT Industry

BSR's membership includes more than 40 of the world's largest and most influential ICT companies. BSR helps its ICT member companies integrate sustainability into their business strategies and governance and address issues of material significance to the sector. BSR played a key role in the founding of both the Global Network Initiative and the Responsible Business Alliance (previously known as the Electronic Industry Citizenship Coalition).

 See more: <https://www.bsr.org/en/industry-focus/information-and-communications-technology>

Contact



Dunstan Allison-Hope
Managing Director
dhope@bsr.org

Resources

GLOBAL NETWORK INITIATIVE

International multi-stakeholder organization that brings together companies, civil society, academics, and investors to protect and advance free expression and privacy.¹⁰

RESPONSIBLE BUSINESS ALLIANCE

A nonprofit coalition of electronics, retail, auto, and toy companies committed to supporting the rights and wellbeing of workers and communities worldwide affected by the global electronics supply chain.¹¹

FREEDOM ONLINE COALITION

A partnership of 30 governments working to advance Internet freedom. Coalition members work closely together to coordinate their diplomatic efforts and engage with civil society and the private sector to support Internet freedom—free expression, association, assembly, and privacy online—worldwide.¹²

PARTNERSHIP ON AI

Established to study and formulate best practices on AI technologies, to advance the public's understanding of AI, and to serve as an open platform for discussion and engagement about AI and its influences on people and society.¹³

¹⁰ <https://www.globalnetworkinitiative.org/>

¹¹ <http://www.responsiblebusiness.org/>

¹² <https://www.freedomonlinecoalition.com/>

¹³ <https://www.partnershiponai.org/>



BSR is a global nonprofit organization that works with its network of more than 250 member companies and other partners to build a just and sustainable world. From its offices in Asia, Europe, and North America, BSR develops sustainable business strategies and solutions through consulting, research, and cross-sector collaboration. Visit www.bsr.org for more information about BSR's 25 years of leadership in sustainability.



Copenhagen | Guangzhou | Hong Kong | New York | Paris | San Francisco | Shanghai | Tokyo