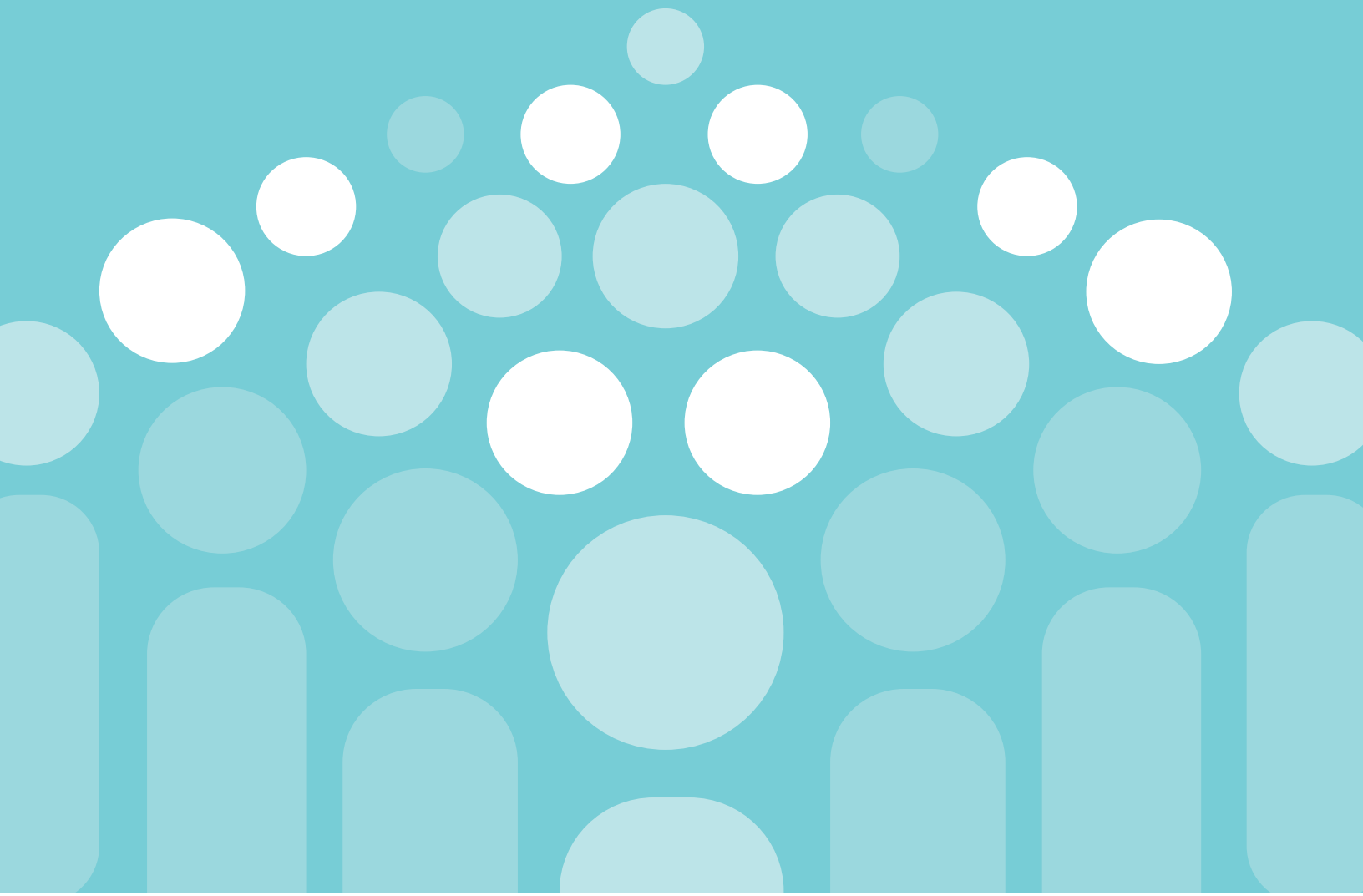

INVESTOR ALLIANCE FOR HUMAN RIGHTS
AN INITIATIVE OF ICCR

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

SALIENT ISSUE BRIEFING:
Freedom of Opinion and Expression

CONTENTS

INVESTOR ALLIANCE FOR HUMAN RIGHTS
AN INITIATIVE OF ICCR

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

SALIENT ISSUE BRIEFING:
Freedom of Opinion and Expression

Freedom of Opinion and Expression (FOE) is a salient human rights issue in the 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.

The ICT sector can promote human rights by enabling open communication between people, empowering them to express themselves as individuals or collectively as groups, and amplifying the voices of historically underrepresented communities. However, the benefits of new communication technologies can be severely undermined when human rights are threatened or violated by their misuse. This may include the use of technology to place illegitimate restrictions on civic space, spread disinformation, unjustifiably surveil certain individuals or groups, and/or censor or otherwise discriminate against people based on their expressed opinions.

INTERNATIONAL STANDARDS

Definitions, instruments, and authorities to consider when conducting human rights due diligence in relation to FOE.

Article 19 of the Universal Declaration of Human Rights (UDHR) states that "[e]veryone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." FOE is also a fundamental human right under Article 19 of the International Covenant on Civil and Political Rights (ICCPR).

As noted in 2018 by the United Nations (UN) Special Rapporteur on the promotion and protection of the right to FOE, "the activities of companies in the ICT sector implicate rights to privacy, religious freedom and belief, opinion and expression, assembly and association, and public participation, among others."

FOE therefore correlates with the rights to privacy and data protection, as stressed by the UN General Assembly in 2013: "the exercise of the right to privacy is important for the realization of the right to freedom of expression and to hold opinions without interference, and is one of the foundations of a democratic society." FOE is also closely related to the rights to peaceful assembly and freedom of association (respectively defined under the UDHR (Article 20) and the ICCPR (Articles 21-22), as these rights enable individuals to organize and express themselves as a community.

The UN Special Rapporteur on FOE has further stated that "distinctive features of the Internet that enable individuals to disseminate information in 'real time' and to mobilize people has also created fear amongst Governments and the powerful. This has led to increased restrictions on the Internet through the use of increasingly sophisticated technologies to block content, monitor and identify activists and critics, criminalization of legitimate expression, and adoption of restrictive legislation to justify such measures."

HOW DO ICT COMPANIES IMPACT FOE IN PRACTICE?

ICT companies can negatively impact the right to FOE in a number of ways, including the following:

- Enabling online harassment such as "doxing" and "trolling," hate speech, and incitement to violence, especially against women (including online stalking, sexual harassment, and "sextortion"), LGBTI people, and other vulnerable users and groups, leading to self-censorship or discouraging individuals from using particular platforms;
- Censoring users at the request of third parties, including governments;
- Enabling government surveillance of private digital networks;
- Blocking access to platforms and websites;
- Lacking due process safeguards or transparency concerning the enforcement of content restrictions;
- Enforcing restrictive legislation, such as laws that criminalize protected speech; and
- Lacking clarity concerning the human rights standards applicable to the development, sale, and use of interception capabilities.

RESOURCES

- Access Now's Freedom of Expression portal contains up-to-date information on FOE worldwide.
- Article 19 promotes media freedom and access to information and protects journalists, human rights defenders, and civic space.
- Authoritarian Tech provides global reporting on how governments abuse and distort the power and potential of emerging technologies.
- Electronic Frontier Foundation champions FOE through litigation, policy analysis, grassroots activism, and technology development.
- Freedom on the Net provides information on internet freedom in 65 countries.
- International Freedom of Expression Exchange publishes daily alerts on FOE.

RANKING DIGITAL RIGHTS

In 2018, the Ranking Digital Rights (RDR) Corporate Accountability Index found that ICT companies do not adequately inform the public about how content and information flow is policed and shaped by their platforms and services. Despite revelations that the world's most powerful social media platforms have been used to spread disinformation and manipulate political outcomes in a range of countries, companies' efforts to police content often lack transparency, grievance processes, and accountability mechanisms.

How does Artificial Intelligence impact conflict and security?

Companies increasingly use AI-powered tools to deploy or enhance their activities. Social media platforms, for example, depend on algorithmic decision-making to rank posts on users' profiles or moderate content. By removing or down-ranking content, from text to images to videos, ICT companies have the power to shape the information that users are exposed to and are thus gatekeepers to the modern-day exercise of FOE.

When content exposing human rights abuses is automatically removed through algorithmic filtering, or activist groups are blocked, people's ability to raise awareness of issues of public interest or to organize is stifled. Furthermore, the expansion and development of bot accounts can exponentially increase online harassment, which typically targets vulnerable groups such as women, further contributing to self-censorship. In addition, governments, especially authoritarian regimes, can use AI-enhanced technology for selective and retroactive censorship through predictive control of potential dissidents. AI-enhanced surveillance, such as face recognition, can also have a chilling effect on FOE as people opt to remain silent for fear of being targeted.

THE 'BUSINESS CASE' FOR FOE

Beyond their human rights responsibilities, ICT companies that do not proactively assess and address FOE risks face potential legal, reputational, and financial risks.

Companies that do not adequately respect FOE rights in their operations and value chains increasingly risk reputational harm, financial loss, shareholder actions, and dissatisfaction among employees, customers, and users. Also, in places where regimes oppress their populations, where the law does not protect FOE, or the justice system does not enforce such guarantees, governments are more likely to limit business opportunities, and companies are more likely to contend with cronyism, bribery, and extortion. According to Freedom House, "governments in countries identified as Not Free in *Freedom in the World* generally impose more red tape, build up barriers to trade, and fail to enforce contracts." In contrast, there is evidence that companies stand to benefit from improved FOE in countries where they operate.

HUMAN RIGHTS GUIDANCE FOR BUSINESS ON FOE

Drawing from UN Guiding Principles on Business and Human Rights, **Ranking Digital Rights** and reports from the Special Rapporteur on FOE, the following human rights due diligence guidance for businesses to prevent, mitigate, and address adverse human rights impacts on FOE aims to help inform investor engagements with ICT companies.

Companies should recognize that the authoritative global standard for ensuring FOE is human rights law.	Companies should, at the highest levels of leadership, adopt and publicly disclose specific policies that direct all business units, including local subsidiaries, to resolve legal ambiguity in favor of respect for FOE and other human rights.
Companies should clearly identify and prioritize real and potential adverse impacts to FOE associated with their operations, products, and/or services.	This includes risks associated with the curation of user feeds and other forms of content delivery; the introduction of new features or services and modifications to existing features and services; the development of automation technologies; and market-entry decisions such as arrangements to provide country-specific versions of the platform. There should be board level oversight of how the company's business operations affect FOE.
Companies should commit to pushing back against excessively broad or extra-legal third-party requests that may impact FOE, including requests from governments.	When faced with problematic requests, companies should seek clarification or modification; request the assistance of civil society, peer companies, relevant government authorities, international and regional bodies, and other stakeholders; and explore all legal options for challenge.
Companies should have in place clear and detailed content moderation policies and processes which respect to users' FOE rights.	Efforts should include strengthening and ensuring professionalization of their human evaluation of flagged content and providing all users with accessible and meaningful opportunities to opt out of platform-driven content curation.
Companies should strengthen transparency and disclosure of policies and processes relevant to FOE, with special attention given to vulnerable groups.	Transparency reports should include information about the circumstances under which content or accounts may be restricted, as well as any government demands and public-private initiatives to restrict online content. Reporting about State requests should be supplemented with data concerning the types of requests received (e.g., defamation, hate speech, terrorism-related content) and actions taken (e.g., partial or full removal, country-specific or global removal, account suspension, removal granted under terms of service).
Companies should map and offer (in coordination with State-based mechanisms) effective remedies for adverse impacts on FOE.	This includes enabling users to challenge content moderation decisions through accessible and effective complaint mechanisms, as well as instituting robust remediation programs (e.g., reinstatement, acknowledgment and settlements related to reputational or other harms).

Supporting activists' efforts to protect freedom of expression

Businesses should seek to collaborate with civil society to tackle challenges associated to FOE. For example, in response to the Russian government's use of antipiracy laws to target dissidents in 2009, and concerns raised by civil society about the company's role in enabling associated abuses, Microsoft pledged to conduct an investigation, develop a temporary free software license, and work to transition to a permanent software donation program for NGOs and small independent media. Also, in 2011, Google submitted a confidential memo to Indian regulators expressing opposition to vague new restrictions on internet content. Effective support requires cultivating strong relationships with advocacy groups and seeking out advice on creative, strategic, and effective ways to address FOE issues across complex value chains.

INVESTOR GUIDANCE FOR ENGAGING ICT COMPANIES ON FOE

The following questions 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 FOE.

- Has the company adopted a public facing policy commitment to respecting human rights, including FOE? If yes, has the commitment been approved at the most senior levels of the company?
- Does the company conduct impact assessments on a regular basis and respond to changing circumstances around FOE? If yes, are these assessments gender-sensitive and do they include meaningful consultation with affected stakeholders, including LGBTQI communities, political dissidents, women, and other vulnerable groups?
- Does board membership include people with expertise on human rights, including FOE, and does the company provide clear evidence of senior-level oversight of FOE risks?
- Are the company Terms of Service consistent with international human rights standards, particularly with regard to FOE? Are these terms publicly available in a language and manner that is clear and accessible for potentially affected stakeholders?
- Does the company have a policy on developing and deploying AI-powered tools in a manner that is consistent with international human rights standards?
- Does the company exercise leverage, such as contractual requirements, commercial incentives, and/or capacity building to help enforce its FOE commitments with regard to business relationships?
- Does the company engage with industry peers to drive shared requirements of business relationships, including governments?
- Does the company disclose clear information about its policies and practices regarding collection, use, sharing, and retention of information that could be used to identify, profile, or track its users?
- Does the company disclose policies for how it handles all types of third-party requests (by authorities or any other parties) to share user data, restrict content, restrict access, or shut down service (including network shutdowns by telecommunications companies)? If yes, do these policies effectively protect user privacy and safety with respect to data transfer requests from third-parties, especially from governments?
- Does the company have safeguards against potential big data misuse by the government?
- Does the company offer accessible and effective grievance and remedy mechanisms, allowing users and other potentially affected rights-holders to notify the company when their FOE rights have been affected or violated in connection with the company's business? If yes, do these policies effectively provide remedy when impacts do occur?

There are a number of tools that can help businesses identify and assess their real and potential impacts human rights, including FOE. These include the "Human Rights Impact Assessment Guidance and Toolbox" by the Danish Institute for Human Rights, and "Doing Business with Respect for Human Rights: Assessing Impacts" by the Global Compact Network Netherlands, Oxfam and Shift. Based on human rights impact assessments, companies such as Google, Twitter, and Facebook have developed policies and procedures to increase transparency around government requests that affect FOE. More tools can be found by clicking here.

INVESTOR EFFORTS

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

- In 2007, New York State Pension Funds submitted a shareholder resolutions at Google and Yahoo calling on them to implement new policies to uphold freedom of speech.
- The GNI Principles on Freedom of Expression and Privacy: These global Principles on Freedom of Expression and Privacy ("the Principles") have been developed by companies, investors, civil society organizations and academics (collectively "the participants") who aim to protect and advance freedom of expression and privacy in the Information and Communications Technology (ICT) industry globally.
- In 2019, a coalition of Google shareholders led by Azzad Asset Management filed a resolution asking the company to publish a human rights impact assessment of its censored search product, "Dragonfly," reportedly for use in China, citing concerns that Google's compliance with China's repressive laws would enable surveillance and censorship, posing human rights risks.
- In the 2019 Investor Alliance for Human Rights' Statement on Corporate Accountability for Digital Rights, investors used their leverage to urge ICT companies to make clear public commitments to respect users' right to FOE, and to disclose their policies affecting users' expression throughout their value chains.

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 four continents and represent $3.5 trillion assets under management. 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

Acknowledgement: We would like to thank Global Partners Digital for their input in the development of this module.