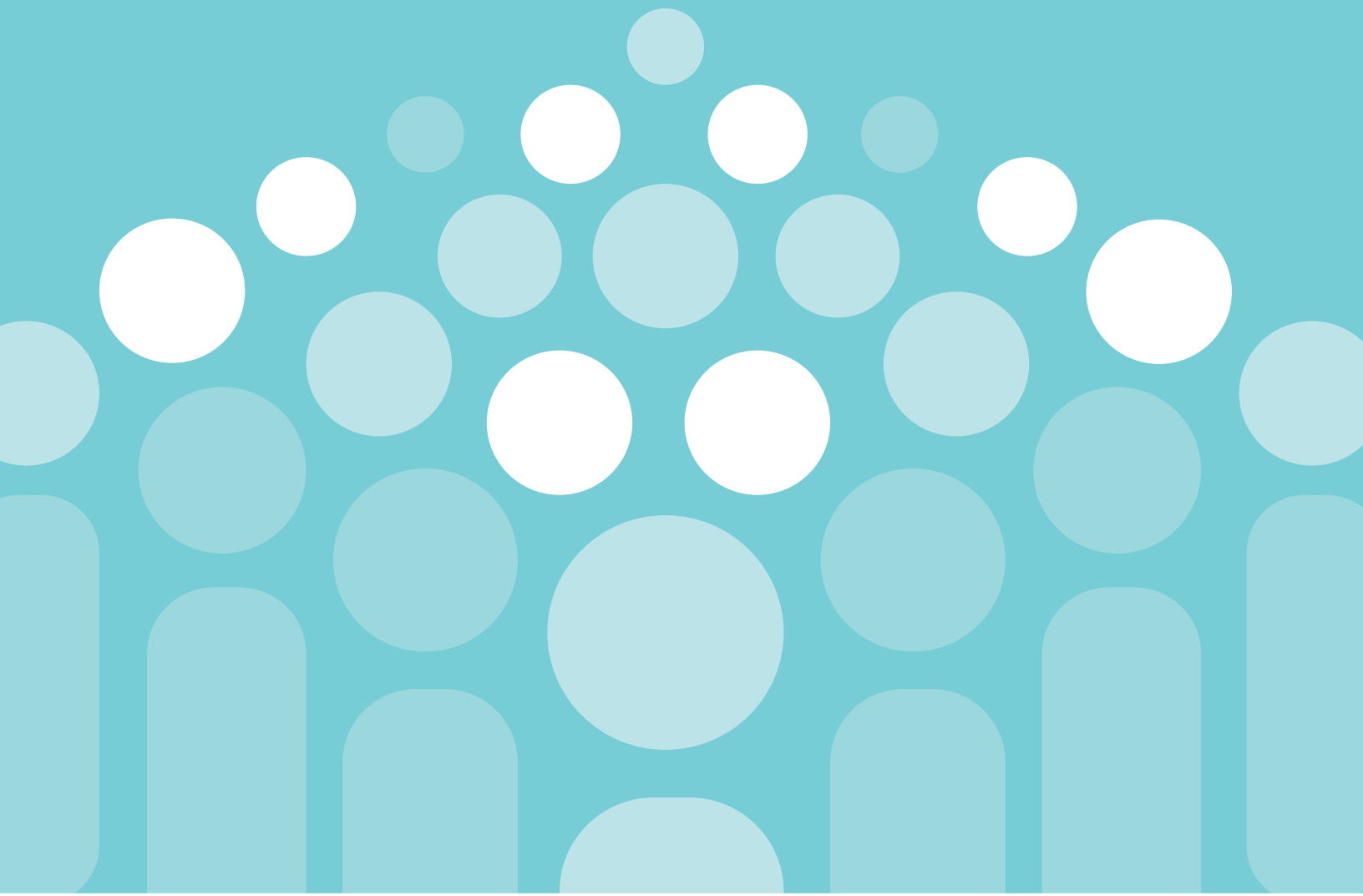

INVESTOR ALLIANCE FOR HUMAN RIGHTS
AN INITIATIVE OF ICCR

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

SALIENT ISSUE BRIEFING: Political Participation

CONTENTS

2 International Standards
3 ICT Impacts on Political Participation
6 The 'Business Case' for Political Participation
7 Human Rights Guidance for Business on Political Participation
10 Investor Guidance on Engaging ICT Companies
11 Investor Efforts

INVESTOR ALLIANCE FOR HUMAN RIGHTS
AN INITIATIVE OF ICCR

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

SALIENT ISSUE BRIEFING:
Political Participation

Political participation 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.

From the industry's earliest days, advances in ICT have promised to contribute to democratization by enabling citizens to have an active hand in how they are governed. ICT promotes sharing of information and enables political expression, participation, and inclusion. Apps that crowd source data allow voters to monitor the fairness of elections. E-democracy encapsulates the use of technology to encourage people's involvement in government. This includes contributing to the development of laws and regulation and enabling political self-determination. ICT has played a central role in efforts to overthrow authoritarian regimes. When used responsibly and accountably, ICT can promote the enjoyment of human rights that support democracy.

Yet the peril of ICT is that it also can be used to disrupt democracies. Governments have deployed ICT to censor and surveil citizens and political opponents. Private user data has been exploited for targeted political advertising. Social media platforms have been hijacked to interfere in elections and have been weaponized to bolster extremism and oppression. The spread of political disinformation undermines trust and social cohesion. At the same time, efforts to moderate and eliminate extremist content and false information can potentially imperil rights to free speech and political participation. Artificial intelligence, if not used accountably, can lead to racial profiling, discrimination, invasion of privacy, and censorship and ultimately hinder certain groups' ability to participate in political processes. Lobbying by ICT companies gives them an outsized voice in political decision-making. Due to gaps in regulation, these potential and actual negative impacts are not being addressed. A smart mix of regulatory guidance and multi-stakeholder ICT self-regulation are needed to close the gaps.

INTERNATIONAL STANDARDS[1]

Definitions, instruments, and authorities to consider when conducting human rights due diligence in relation to political participation and other salient human rights issues.

According to the United Nations (UN) Office for the High Commissioner of Human Rights, "Democracy is one of the *universal core values and principles of the United Nations.*" Several UN Human Rights Council resolutions emphasize the mutually reinforcing relationship between democracy and human rights. The Universal Declaration of Human Rights (UDHR) details political rights and civil liberties which are essential for democracy and find further elaboration in the International Covenant on Civil and Political Rights (ICCPR). Central among them is the right to political participation. Article 21 of the UDHR and Article 25 of the ICCPR establish that everyone has the right "to take part in the conduct of public affairs, directly or through freely chosen representatives," that the "will of the people shall be the

basis of the authority of government," and that "this will shall be expressed in periodic and genuine elections which shall be by universal and equal suffrage."

The right to political participation can only be enjoyed if other rights such as the right to non-discrimination (UDHR Article 2), freedom of opinion and expression, which includes the freedom to "seek, receive and impart information and ideas through any media and regardless of frontiers" (UDHR Article 19), the right to freedom of peaceful assembly and association (UDHR Article 20), and the right to privacy (UDHR Article 12) are upheld. In a 2013 resolution the UN General Assembly reaffirmed the correlation between rights, "recognizing that 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" and "stressing the importance of the full respect for the freedom to seek, receive and impart information, including the fundamental importance of access to information and democratic participation." Previous briefings explore in depth how the ICT sector impacts on freedom of expression, the right to privacy, and the right to non-discrimination.

The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression remarked in 2018 that, "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." In keeping with the UN Guiding Principles on Business and Human Rights (UNGPs), the Special Rapporteur encouraged companies to "apply human rights standards at all stages of their operations" and to "articulate their positions in ways that respect democratic norms and counter authoritarian demands." This briefing focuses specifically on how the ICT sector can impact the right to political participation as a foundation for strong democracies.

HOW DO ICT COMPANIES IMPACT POLITICAL PARTICIPATION IN PRACTICE?

Freedom on the Net, the 2018 report from Freedom House, describes a rise in "digital authoritarianism" with the decline of global internet freedom for eight consecutive years. The report warns that the internet and its associated technologies can be disruptive to democracies. Trends relating to the spread of disinformation and polarization of political discourse, misuse of user data, censorship, and automated surveillance demonstrate that democratic institutions and basic rights may be endangered.

ICT companies can negatively impact the right to political participation in several ways, including:

- Enabling the surveillance of political opponents, activists, marginalized groups and others with the intent of silencing political opposition by, for example, denying internet access (e.g. Egypt blocking access to social media and news sites during demonstrations; Israel's deployment of Cisco Systems' surveillance technology in OPT; Turkey's use of FinFisher malware to spy on opposition protestors; use of facial recognition technology to target Uighurs).

RESOURCES

- Department of State, Draft U.S. Government Guidance for the Export for Hardware, Software and Technologies with Surveillance Capabilities and/or Parts/Know-How provides guidance to assist exporters of items with intended and unintended surveillance capabilities with implementation of their human rights responsibilities in line with the UNGPs and OECD Guidelines.
- Council of Europe, Algorithms and Human Rights examines a number of human rights concerns triggered by the increasing role of algorithms in decision-making.
- AI Now is a research institute at New York University examining the social implications of artificial intelligence, to include on rights and liberties.

continued on next page

- Failing to protect personal user data and social media platforms from being utilized to affect electoral outcomes (e.g. final report of the Senate Intelligence Committee detailing Russian interference into the 2016 presidential election; NYU Stern Center for Business and Human Rights warns of disinformation in the 2020 elections).
- Allowing the spread of disinformation which undermines confidence in political institutions and traditional media outlets, creates confusion around public affairs, and polarizes societies by undermining trust and social cohesion (e.g. concerns raised at EC High Level Hearing, Preserving Democracy in the Digital Age; Facebook suspends Russian accounts accused of meddling in domestic politics of eight African countries; use of 'deepfakes' to malign political opponents).
- Failing to halt the weaponization of social media platforms to bolster extremism and oppression at a time when violence attributed to hate speech has increased world-wide (e.g. Facebook used to incite violence against Rohingya; online sexist and racist harassment has chilling effect on political participation and can lead to self-censorship; livestreaming of attacks and posting of manifestos; social media used to build support for Sudanese government)
- While at times platforms fail to moderate content, such as hate speech, in other instances they are aggressively moderating content, censoring and silencing certain political viewpoints and protected speech (e.g. Twitter announces ban on all political advertising; TikTok's local moderation guidelines discriminate against LGBTQ content; forms of prior restraint and removal of lawful content to avoid liability).
- Developing digital identity programs that may result in denial of access to government services, misuse of information for surveillance purposes, and violation of the right to privacy.
- Lobbying to increase influence on political decision making (e.g. 2018 marks highest level of lobbying expenditures with possible regulation of privacy, election security, and antitrust matters).

- The IEEE's Global Initiative on Ethics of Autonomous and Intelligent Systems has released an updated public consultation draft of Ethically Aligned Design: A Vision For Prioritizing Human Well-being with Autonomous and Intelligent Systems.
- The International Institute for Democracy and Electoral Assistance's (IDEA) initiative on ICT, Elections & Democracy produces research and maintains a database of ICTs' use in elections.
- The Brennan Center for Justice's program, Defending our Democracy, produces research and advocates for improved election security.
- OpenMIC works with impact investors to advocate for greater corporate accountability for ICT companies in the areas of openness, equity, privacy, and diversity.
- Access Now's Keep It On Coalition tracks and advocates against internet shutdowns around the world.
- It's Not Just the Content, It's the Business Model: Democracy's Online Speech Challenge by Ranking Digital Rights

How does Artificial Intelligence impact political participation?

Artificial intelligence (AI) and the underlying algorithms and data sets that enable high-speed computational decision-making on a large scale can have significant impacts on an array of human rights. In particular, the right to political participation depends on an information environment where people have unfettered access to accurate information and can engage freely in political discourse and activities, individually and in association with others, without fearing discrimination, surveillance, and reprisals. While AI can enable political participation, there are certain risks associated with automation, data analysis, and adaptability. For example, automated decision-making may rely on datasets that reproduce discriminatory effects, and overreliance on non-transparent algorithms may limit the ability to scrutinize outcomes and access remedy. The use of data sets containing personal data raises concerns about their origins, accuracy, and individuals' rights over the information. Machine-learning AI systems are adaptable, but increasingly eliminate humans from defining objectives and outputs of an AI system, making it challenging to foresee and mitigate adverse human rights impacts. That said, human agency is central in the development of datasets and algorithms and determines the application of AI and the use of its outputs. ICT companies have a responsibility to ensure that AI is not applied in a fashion that harms human rights and undermines the institutions central for strong democracies.

There are three applications of AI in the information environment that raise concerns, including for the right to political participation.

- **Content display and personalization:** Algorithms that rank and curate information to offer users increasingly personalized experiences may limit exposure to content not deemed engaging to the user, thereby eliminating access to politically diverse views as users find themselves in echo chambers. Personalization may reinforce biases and promote exposure to inflammatory content.
- **Content moderation and removal:** AI can assist companies with moderating and removing content in accordance with terms of service and in response to government requests. However, algorithms may be challenged in assessing the context of content, may be grounded in datasets that incorporate discriminatory assumptions, and may result in the removal of legitimate content. Some degree of human content moderation is needed to avoid a chilling effect on political discourse.
- **Profiling, advertising, and targeting:** Increasingly, consumers and voters are micro-targeted through the collection and exploitation of their personal data. Yet targeted advertising can increase the risk of manipulation of users through the spread of disinformation masquerading as legitimate news, perpetuate discrimination, influence electoral processes, and suppress voter turnout. Algorithms can exclude users from access to information, essential social services, and opportunities. According to the Special Rapporteur on freedom of opinion and expression, microtargeting is "creating a curated worldview inhospitable to pluralistic political discourse." Debates have ensued on how to best ensure truthful paid political advertising while upholding rights to political expression.

The dilemma of addressing false political content

Recognizing that political disinformation can pose a threat to election integrity and democratic institutions, what is the appropriate corporate response?

In the absence of clear regulatory guidelines, ICT companies have taken varying approaches, from Twitter announcing it will ban all political advertising (electioneering ads and those related to political issues), to Facebook exempting political ads from bans on making false claims. Facebook's announcement met with strong criticism, but CEO Mark Zuckerberg defended his position, citing the need to protect freedom of expression and questioning whether it is appropriate for "a private company to censor politicians or the news in a democracy." While Twitter and Facebook appear to be holding antithetical positions, in practice social media companies respond inconsistently to false political content on their platforms. Nevertheless, the central dilemma for ICT companies and government authorities will be allowing first amendment protected free speech, while simultaneously keeping hate speech and misinformation

campaigns in check." While some research advocates for the removal of "provably false information," others seek to avoid "censorship-based approaches" and social media companies serving as "arbiters of truth."

Consensus seems to be emerging among legislators, academics, and other stakeholders that it is time to have a public dialogue about a "new social contract with technology." Central to this discussion is whether the business model of social media platforms, which draws revenue from applying AI to user data to enable targeted paid advertising, "intentionally bypasses the marketplace of ideas." As Facebook's employees have pointed out, "free speech and paid speech are not the same thing."

While legislative proposals are, among other things, pushing for greater disclosure around paid political advertising, akin to those required of other traditional media platforms, this does not address the dilemma related to truth in political content and other regulatory gaps. Therefore, some are pushing for a comprehensive smart mix of ICT self-regulation and government policies "rooted in transparency, privacy and competition" that can address the root causes of political disinformation as exacerbated by the business model of ICT platforms. Some companies, such as Facebook, have publicly welcomed regulatory guidance on privacy, political advertising, and moderation of harmful content.

THE 'BUSINESS CASE' FOR POLITICAL PARTICIPATION

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

ICT companies have positive and negative incentives to address risks to political participation and associated rights in their operations and value chains. For example, responsible companies are more likely to attract top talent. Conversely, when employees believe their company is contributing to human rights harms, they may resign or disrupt operations through strikes and other actions, as Google employees did when they learned of project Dragonfly to develop censored search engines for China. Companies can proactively address potential human rights risks, such as those linked to facial recognition technology, with government and other stakeholders or potentially face regulatory scrutiny. With regulatory action appearing increasingly inevitable, companies will benefit from embracing transparent and accountable business practices and collaboratively shaping regulations. Positive brand image is key to corporate financial success, and damage to corporate reputation can be extremely costly. Facebook learned this lesson when, in the wake of the Cambridge Analytica data breach and election interference scandal, the company experienced the largest stock market value drop in history, an advocacy campaign urged users to delete their accounts, and the D.C. attorney general sued for lax privacy standards violating consumer protection laws. ICT companies' alleged misuse of user data has opened the door to numerous lawsuits which pose significant legal and financial risks.

HUMAN RIGHTS GUIDANCE FOR BUSINESS ON POLITICAL PARTICIPATION

Drawing from the UN Guiding Principles on Business and Human Rights, the ICT Sector Guide on Implementing the UN Guiding Principles, reports from the Special Rapporteur on freedom of expression (A/73/348 and A/HRC/38/35), and Ranking Digital Rights draft Best Practices on Targeted Advertising and Algorithms, Machine Learning, and Automated Decision-making, the following guidance for businesses to prevent, mitigate, and address adverse impacts on political participation aims to help inform investor engagement with ICT companies. Relevant previous guidance on the right to privacy, freedom of expression, security, and discrimination is not replicated here.

UNGPs	Implementation	Good Practice Examples
Develop a policy commitment and embed respect for human rights	Companies should (with relevant expert and stakeholder input) develop a publicly available human rights policy commitment that recognizes international human rights law as the authoritative standard for the right to political participation. The commitment should be approved at the highest levels of management; communicated internally; embedded in all business policies and processes as well as products, services and technologies ("human rights by design"); and applied to business relationships.	→ Companies should establish in corporate policies and technical guidance to all personnel involved in the AI life cycle (design, deployment, and implementation) that human rights responsibilities guide all business operations. → Companies should communicate their commitment to business relationships, including users, customers, and other business relationships through terms of service or contracts that are aligned with human rights standards and law. → The commitment should identify key human rights risks that may impact on political participation and cross-reference policies detailing the approach to managing those risks, e.g. relating to algorithmic content curation and moderation, third-party targeted advertising, and lobbying. → Companies should strive for coherence between their responsibility to respect human rights and policies that govern their wider business activities and relationships, to include those that address lobbying activities with human rights impacts.
Assess real and potential human rights impacts	Companies should assess (in consultation with affected stakeholders and drawing on relevant expertise) actual and potential negative human rights impacts linked to their operations and technological products and services, including those linked to their business relationships throughout the value chain. The focus should be on salient risks to people, especially vulnerable and marginalized groups, and not solely to the company.	→ Risk assessment should be an ongoing process, conducted for new markets, business relationships, and technological applications, e.g. of surveillance, 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 discrimination, surveillance, and political repression related to facial recognition technologies or risks to freedom of expression and information, privacy, and political participation linked to targeted political advertising.

continued on next page

Integrate and act on findings of assessments	Using the results of the human rights risk assessment, companies should integrate the findings across relevant internal functions and processes (with clear assignment of roles, responsibilities, and resources); prioritize impacts for action based on their severity (scale, scope and remediability); and identify options to prevent or mitigate impacts. The ability of a company to address impacts will depend on whether it causes, contributes to, or is directly linked through a business relationship to impacts. Companies should seek to increase and utilize their leverage to address impacts linked to business relationships.	→ According to the Special Rapporteur on freedom of expression, "radical transparency, meaningful accountability and a commitment to remedy" are necessary to protect the use of online platforms for engagement in public life. For example, actions to counter disinformation in political advertising should entail such things as: → Publicly disclosing and inviting stakeholder input into policies; eliminating false and signaling trustworthy content; → De-monetizing disinformation; revealing sponsors of political ads and targeting parameters; → Limiting narrow segmentation of markets; and → Allowing users to opt out of algorithmic content curation. → Companies can increase their leverage to eliminate violent, extremist, and terrorist content by engaging in collaborative action, for example participating in the Global Internet Forum to Combat Terrorism (although care should be given to ensure transparency around content removal and appeals processes).
Track performance	Companies should track their responses to negative impacts to evaluate if they are effectively being addressed, including in business relationships. Progress should be tracked using appropriate quantitative and qualitative indicators and should draw on feedback from internal and external stakeholders.	→ Companies should monitor 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. → In relation to targeted political advertising, monitoring can occur in part through third-party oversight of advertising content and ad targeting parameters. → In relation to algorithmic curation and content moderation, companies can share information about the functionality of algorithms and datasets used to train machine learning models with external researchers who can assess discrimination at the input and output levels.

continued on next page

Communicate performance	While human rights assessment and performance tracking is about 'knowing' a company's human rights impacts, communicating performance is about 'showing' to stakeholders that impacts are being addressed. Communication of progress should occur on a regular basis and be in a form accessible to target audiences. Formal reporting should occur where risks of severe impacts exist.	→ For users and other stakeholders to understand the impact of AI systems on human 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 personal user data will become part of a dataset and how it will be used. → For moderated content, companies should share data, for example, on trends in content display; content removals and the policies and decision processes guiding removals; and how often and on what grounds removals are appealed and responses to appeals. The Santa Clara Principles on Transparency and Accountability in Content Moderation outline three principles for platforms: 1. Numbers (transparency around removals and suspensions), 2. Notice (inform users about take-downs and suspensions) and 3. Appeal (appeals processes for users). → Information on political advertising should include among other things disclosure about the sources and beneficiaries of advertising; targeting parameters used; and actions taken to restrict advertising content or accounts and the policies and reasoning behind those actions.
Remediate	When companies cause or contribute to negative human rights impacts, they must provide or participate in mechanisms which allow for the filing of grievances and remediation of harms. Grievance mechanisms can be operational-level or external to the company, however they must meet certain criteria of effectiveness. Outcomes of the grievance mechanism should flow into risk assessment processes.	→ Users should have access to remedies for the adverse impacts of AI systems. Companies should put in place systems of human review to respond to complaints in a timely manner. Data on the subject and frequency of complaints and requests for remedies, as well as the types and effectiveness of remedies should be published regularly. → Users should have access to a mechanism to appeal the restriction of their content to a human being. Data about the volume and nature of appeals of content moderation decisions and the actions taken in response to those appeals should be disclosed regularly.

Multi-stakeholder engagement to ensure respect for political participation

The ICT sector should work with investors, governments, rights-holders, civil society organizations, and other stakeholders to find ways to identify and address their actual and potential human rights impacts, to include on political participation. With regulatory discussions happening at national, regional, and international levels, ICT companies benefit from proactively working to shape good regulatory outcomes.

Some multi-stakeholder efforts focus on the issues of countering extremist content and AI. For example, companies in the Global Internet Forum to Counter Terrorism (GIFCT) work with governments and civil society to tackle extremist and violent content on their platforms. Among other things, GIFCT shares knowledge of current leading practices around counterterrorism and has created the Hash Sharing Consortium, which shares hashes (i.e. digital fingerprints) of known terrorist images and videos to expedite their removal. However, some experts and NGOs have warned that loose, and at times overly narrow, definitions of terrorist content and lack of transparency on decision-making around removals, deleted content, and appeals could infringe on democratic values and human rights. UNESCO's Internet Universality ROAM-X Indicators enable states, companies, and other stakeholders to assess their national internet environment by measuring human Rights, Openness, Accessibility and Multi-stakeholder participation (ROAM) to, among other things, map and improve the ecosystem in which AI is developed, applied, and governed. The Partnership on AI (PAI) is a multi-stakeholder organization that brings together companies building and utilizing AI technology, academics and experts, civil society organizations, and other stakeholders to better understand AI's impacts, formulate good practices in AI technologies, and serve as a forum to engage on AI and its influences on people and society.

INVESTOR GUIDANCE FOR ENGAGING ICT COMPANIES

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 the right to political participation.

Human rights commitment and governance

- Has the company adopted a public-facing policy commitment to respect human rights, including the right to political participation? If yes, was the commitment developed with expert and stakeholder input and has the commitment been approved at the most senior levels of management?
- How does the company's board ensure it has the appropriate human rights expertise, including political participation and associated rights? How does the company provide senior-level oversight of risk management systems?
- Do the company's terms of service reflect this commitment and is it consistent with international human rights standards? Are these terms publicly available in a language and manner that is clear and accessible for potentially affected stakeholders?

Embedding commitment internally

- How does the company identify risks to people in its own operations and through its business relationships (e.g., human rights impact assessments, conducted on an ongoing basis and in response to changes in risk factors)? Do assessments involve meaningful consultation with affected rights-holders, including the most vulnerable and marginalized populations?

- How does the company assess whether its impacts on political participation undermine confidence in democratic institutions or processes? What steps is the company taking to prevent, mitigate, and account for such impacts?
- Does the company have policies on developing and deploying AI-powered tools in a manner that is consistent with international human rights standards? Do human rights considerations factor into all business operations throughout the AI life cycle and is there a clear assignment of roles, responsibilities, and resources for implementing human rights commitments?

Embedding commitment in relationships

- Does the company communicate its human rights commitment throughout its value chain? Does the company exercise leverage to help uphold its commitment to political participation and associated rights in its business relationships? Where leverage is limited does it seek to increase its leverage, to include in partnership with industry peers and other stakeholders?
- Does the company communicate to users its policies for technologies, services, and products that could pose risks to the right to political participation, such as on targeted political advertising and the use of algorithms, machine learning, and automated decision-making for purposes of content curation, recommendation, and moderation? Does it share data about the implementation and outcomes of those policies, in particular in relation to content removal?
- Does the company have safeguards against potential misuse of its technology by non-state actors (e.g., political hackers), including limiting risks of voter manipulation and election interference? Does it have safeguards against the potential weaponization of platforms to propagate violent and extremist content?

Disclosing how salient human rights issues are addressed

- Does the company disclose information about how it addresses its salient human rights issues in a manner that is accessible to stakeholders, including those whose rights to political participation have been negatively impacted? Does the information allow stakeholders to assess the adequacy of the company's measures to address impacts?

Ensuring access to remedy

- Does the company provide or participate in timely, accessible, and effective grievance mechanisms to offer affected rights-holders access to remedy when their right to political participation and associated rights have been harmed? Does the company periodically assess and disclose information about the effectiveness of the mechanisms?
- Does the company proactively notify users when they believe a harm has occurred?
- Does the company recognize that, in the context of political participation, harms to an individual may have a negative impact on those that witness the harm (chilling effect)? Have they taken remedial steps in this regard?

INVESTOR EFFORTS

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

- In the 2020 proxy season, Newground Social Investment and As You Sow Foundation filed a resolution calling on Facebook to "delete all political ads containing lies and mistruths based on Facebook employee recommendations to avoid adverse impact on our political system… Publicly agree to a policy stating that Facebook will abide by campaign advertising rules like all U.S. broadcasters and end micro-targeting of groups smaller than 5,000 people…Provide full transparency of the Reboot process including listing deleted political ads, bots, fake accounts, fake news, deep fakes and accounts closed," among other things.
- Global investors called on Alphabet, Google's parent company, to establish a Human Rights Oversight Committee of the Board of Directors in a resolution filed in the 2020 season. Investor co-leads—The Sustainability Group of Loring Wolcott and Coolidge, Robeco, Hermes, and NEI Investments—cite concerns

over the company's role in facilitating disinformation and incitements to violence through algorithms that show user-targeted content, among other things.

- In the 2020 proxy season, Nathan Cummings filed a proposal urging the Board of Directors of Facebook to provide oversight of civil and human rights risks citing concerns over the Russian influence campaign undertaken using that platform's targeted advertising during the 2016 U.S. presidential elections to explicitly target African Americans.
- In the 2019 proxy season, Investor Advocate for Social Justice (formerly known as the Tri-State Coalition for Responsible Investment) and Open Mic requested that the Amazon.com board stop the sale of facial recognition technology ('Rekognition') unless an independent evaluation concludes that it will not result in actual or potential negative civil and political human rights impacts, especially if sold to repressive governments.
- Alphabet was also subject of a resolution in 2018 focused on disclosing policies and procedures for making political contributions and expenditures as well as the amounts of monetary and nonmonetary political contributions or expenditures that could not be deducted as an "ordinary and necessary" business expense.
- Azzad Asset Management filed a shareholder resolution in 2019 requesting that Google parent company Alphabet, Inc. publish a Human Rights Impact Assessment examining the actual and potential impacts of censored Google search engines in China.
- In the 2019 proxy season, Sum of Us filed a resolution with Facebook asking that it create a Risk Oversight Board Committee because of its failure to systematically address various risks including its role in proliferating "fake news", targeted advertising to users with offensive content, concerns over censorship in Myanmar and India, and use of the platform to incite terrorism.
- In 2019, NorthStar Asset Management filed a resolution with Intel Corporation calling for the adoption of policy to provide greater disclosure round political contribution expenditures.

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

Developed by the Investor Alliance for Human Rights.