FOC Joint Statement on Spread of Disinformation Online

1. The issue

The members of the Freedom Online Coalition (FOC) are deeply concerned about the growing spread of disinformation[1] online, which can undermine the enjoyment of human rights[2] and public health worldwide. It can hinder freedom of opinion and expression, protection against discrimination , and the open exchange of information necessary for democracy to flourish. Disinformation is growing in scope and sophistication at a time when people all over the world increasingly turn to the Internet to connect, learn and consume their news.

Disinformation can erode public trust in democratic processes and institutions, and undermine public health initiatives. It may further marginalize voices from persons belonging to minorities, fracture community cohesion, polarize societies and incite discrimination, xenophobia, intolerance and violence.

Disinformation can be used to intimidate and harass public figures such as journalists and human rights defenders[4], and target and discriminate against vulnerable persons and groups. We have seen that online disinformation targeting marginalized groups in some cases has even been a precursor to crimes against humanity and other gross violations or abuses of human rights.

Globally, there is evidence that disinformation is employed by state and non-state actors with political, ideological, commercial or other motives, including violent extremist and terrorist groups. Online disinformation campaigns by state and state-sponsored actors can also be used as part of hybrid influence campaigns that aim to destabilize societies.

Future technological developments will continue to exacerbate the online disinformation threat, as well as provide possible solutions to these challenges. Online disinformation campaigns may seek to use certain technologies to drive polarization and negatively impact the ability to share, receive and Impart ideas and misinformation. For example, the use of algorithms to promote certain content can lead to the amplification and prioritisation of targeted disinformation. There is also the potential for emerging technologies to facilitate the creation of increasingly manipulated content, including "synthetic media"6.
The FOC commits to address disinformation while ensuring a free[7], open, interoperable, reliable and secure Internet in which a diversity of voices is heard, and in full respect of human rights. It is therefore important that any measures taken to address disinformation are in accordance with international law, including international human rights law. The FOC is concerned that some states use the guise of countering disinformation to assert excessive control over the Internet, while disregarding international human rights law and principles of a free, open, interoperable, reliable and secure Internet.

The FOC highlights that the Internet should be conducive to a news and media ecosystem where there is access to information and plurality of the media; free and independent media has a sustainable future, and public service media and local news outlets are able to thrive. Public access to factual and diverse information can make societies more resilient to disinformation.

[1] Disinformation is defined here as the deliberate creation and dissemination of false and/or manipulated information that is intended to deceive and mislead audiences, either to cause harm or for personal, political or financial gain.

[2] Disinformation can undermine many human rights including — freedom of opinion and expression [Art 19 ICCPR]; the right to take part in the conduct of public affairs and to vote in elections [Art. 25 ICCPR]; protection against discrimination [Art 2 and 26 ICCPRI; protection of honour and reputation [Art. 17 ICCPR]; the right to health [Art. 12 ICESCRI; the right to education [Art. 13 ICESCRI.

[3] Discrimination is defined by distinction by characteristics including, without limitation: ethnic, national or social origin, religion or belief, political or any other opinion, disability, age, sexual orientation, and gender identity and those who can be vulnerable to multiple and intersecting forms of discrimination.

[4] In the FOC Joint Statement on Defending Civic Space Online, we expressed our concem about shrinking civic and democratic spaces online as a result of state-sponsored obstruction of free expression, peaceful assembly, and free association.

[5] Hybrid influence can be described as influence activities by states and non-state actors that are targeted towards vulnerabilities of societies.

[6] Synthetic media is defined here as audio or visual content that has been manipulated using advanced software to change how a person, object or environment is presented.

[7] "Free" in this context does not mean 'free of cost".

The FOC urges all stakeholders, including governments worldwide, the private sector, civil society, research and educational institutions, the media, and individuals to share experiences, expertise and best practices on addressing disinformation. Such collaboration and engagement will encourage a global movement towards countering disinformation while fully respecting human rights and promoting the multi-stakeholder Internet governance.

2. Call to action

The FOC calls on governments to:

- Abstain from conducting and sponsoring disinformation campaigns, and condemn such acts.
- Address disinformation while ensuring a free, open, interoperable, reliable and secure Internet, and fully respecting human rights.
- Improve coordination and multi-stakeholder cooperation, including with the private sector and civil society, to address disinformation in a manner that respects human rights, democracy and the rule of law.
- Implement any measures, including legislation introduced to address disinformation, in a manner that complies with international human rights law and does not lead to restrictions on freedom of opinion and expression inconsistent with Article 19 of the International Covenant on Civil and Political Rights.
- Respect, protect and fulfill the right to freedom of expression, including freedom to seek, receive and impart information regardless of frontiers, taking into account the important and valuable guidance of human rights treaty bodies.
- Refrain from discrediting criticism of their policies and stifling freedom of opinion and expression under the guise of countering disinformation, including blocking access to the Internet, intimidating journalists and interfering with their ability to operate freely.
- Support initiatives to empower Individuals through online media and digital literacy education to think critically about the information they are consuming and sharing, and take steps to keep themselves and others safe online.
- Take active steps to address disinformation targeted at vulnerable groups, acknowledging, in particular the specific targeting of and impact on women and persons belonging to minorities.
- Support international cooperation and partnerships to promote digital inclusion 8, including universal and affordable access to the Internet for all.

[8] See more detailed: FOC Joint Statement on Digital Inclusion.

The FOC urges social media platförms and the private sector[9] to:

- Address disinfOrmation in a manner that is guided by respect for human rights and the UN Guiding Principles on Business and Human Rights [10].
- Increase transparency into the täctors considered by algorithms to curate content feeds and search query results, formulate targeted advertising, and establish policies around political advertising, so that researchers and civil society can identity related implications.

- Increase transparency around measures taken to address the problems algorithms can cause in the context of disinformation, including content take down, account deactivation and other restrictions and algorithmic alterations. This may include buildmg appropnate mechanisms tor reportmg, designed 111 a multi-stakeholder process and without compronusmg effectiveness or trade secrets.
- Promote users' access to meanmgful and timely appeal processes to any decisions taken m regard to the removal of accounts or content.
- Respect the rule of law across the societies 111 which they operate, while ensurmg not to contribute to violations or abuses of human rights.

- Use Independent and Impartial fäct-checkmg services to help identify and highlight disinformation, and take measures to strengthen the provision of independent news sources and content on their platforms.
- Support research by working with governments, civil society and academia and, where appropriate, enabling access to relevant data on reporting, appeal and approval processes, while ensuring respect for international human rights law.

The FOC urges civil society and academia to:

- Continue research into the nature, scale and impact of online disinformation, as well as strategic level analysis to inform public debate and government action.
- Adequately consider the impact of disinformation on women and marginalized groups who are targeted by disinformation campaigns in this research.
- Engage with the private sector and governments to share findings and collaborate on research, whilst ensunng appropriate privacy protections are in place.
- Actively participate in public debate and in multi-stakeholder initiatives looking to address disinformation and emphasize the necessity of evidence-based discussion.

---

[9] Relevant actors include companies that permit the sharing of and other interactions with user generated content and those which have involvement in shaping the presentation of content to users (e.g. search engines).

[10] United Nations, Guiding Pnnciples on Business and Human Rights, 2011https:/,mwvv.ohchr.org/documents/publications/guidingprinciplesbusinesshr en.pdt

FOC Joint Statement on COVID-19 and Internet Freedom

The Freedom Online Coalition (FOC) is a group of 31 countries deeply committed to the promotion and protection of human rights and fundamental freedoms proclaimed in the Universal Declaration of Human Rights (UDHR). We believe that the human rights and fundamental freedoms that individuals have offline must also be protected online. We are committed to working together to support Internet freedom for individuals worldwide – including the freedoms of expression, association, peaceful assembly, as well as privacy rights online.

The FOC shares the concerns of people everywhere in the face of the COVID-19 global pandemic, including the negative economic impact associated with it, and recognizes government efforts to mitigate the spread of the virus
by enacting emergency measures. At the same time, more activities are taking place online than ever before, and we are concerned with the human rights implications of certain measures, practices, and digital applications introduced by governments in response to the crisis. This includes the use of arbitrary or unlawful surveillance practices; partial or complete Internet shutdowns; online content regulation and censorship that are inconsistent with human rights law. We are further concerned with the potential short-and-long-term impact of these actions on the rights of freedom of expression, association, and peaceful assembly, and privacy rights, even after the pandemic is over.

Lack of accountability and lack of effective remedy for violations and abuses of human rights online pose a risk of reduced trust in public authorities, which, in turn, might undermine the effectiveness of any future public response. Violations and abuses of human rights also increase risk of discrimination and may disproportionately harm members of already marginalized and vulnerable communities, including women and girls and other individuals who may face multiple and intersecting forms of discrimination. Human rights violations and abuses online are a direct challenge to the FOC's goal of protecting and promoting both the exercise of human rights online and an open, free[1], secure, reliable, and interoperable Internet.

Furthermore, the FOC is concerned by the spread of disinformation online and activity that seeks to leverage the COVID19 pandemic with malign intent. This includes the manipulation of information and spread of disinformation to undermine the international rules-based order and erode support for the democracy and human rights that underpin it. Access to factual and accurate information, including through a free and independent media online and offline, helps people take the necessary precautions to prevent spreading the COVID-19 virus, save lives, and protect vulnerable population groups.

We reiterate that commitments and principles outlined in FOC founding documents remain of the utmost importance. We further emphasize that countries must ensure that measures implemented to address the pandemic are in compliance with international human rights law. Measures should also be limited to what is necessary for the legitimate protection of public health, including by limiting these measures in time only as necessary to address the COVID-19 crisis. Any interference with privacy and other relevant rights and freedoms need also be consistent with the International Covenant on Civil and Political Rights and the UDHR. This is true whether the restrictions apply to activity online or offline. We welcome the focus on this issue by the UN Secretary General, the UN High Commissioner for Human Rights, and UN Special Rapporteurs and experts.

In response to the COVID-19 pandemic, we call upon governments worldwide:

- To refrain from adopting or implementing laws and policies that may negatively affect the enjoyment of human rights, or that unreasonably restrict civic space online and offline, in violation of states' obligations under international human rights law;

- To promote an enabling environment for free expression and access to information online to protect privacy and to
refrain from content restrictions that violate international human rights law;

- To take appropriate measures to counter violence, intimidation, threats and attacks against individuals and groups, including human rights defenders, on the Internet and through digital technologies;

- To immediately end Internet shutdowns, and ensure the broadest possible access to online services by taking steps
to bridge digital divides; and

- To commit that any actions taken pursuant to emergency measures or laws be subject to effective transparency and accountability measures and lifted when the pandemic has passed.

...while committing ourselves to do the same.

FOC Joint Statement on Digital Inclusion

3. The Issue

In an increasingly digitized world, Information and Communication Technologies (ICTs), in particular the Internet, offer countless opportunities: facilitating the acquisition of knowledge and skills, creating financial opportunities, enhancing communication and more. ICTs are a vital component of social and economic advancement, especially in developing countries. In addition, the Internet and ICTs provide a unique platform that enables individuals to exercise their human rights more fully. They are an important tool for human rights defenders as affirmed in the FOC's Joint Statement on Defending Civic Space Online. For instance, the Internet and ICTs allow people to express and exchange opinions and thoughts freely, gather information, participate in democratic processes and organize public protests as well as advocacy campaigns.

However, a persisting lack of digital inclusion prevents people from realizing the full potential and benefits provided by the Internet and thereby creates digital divides. These digital divides are plural because discrepancies in access exist across demographics and abilities, including geography, area/location, gender, class, ethnic background and differently abled individuals. Moreover, a lack of digital inclusion also affects those who already are connected, often preventing a full or meaningful use of the Internet. While the Internet and ICTs have the potential to empower marginalized groups, it also carries the risk of reinforcing existing social and economic inequalities, particularly impacting already marginalized or vulnerable groups: a tendency which appears particularly serious in times of ubiquitous digitalization.

There is a growing awareness of the problems posed by a lack of digital inclusion, as highlighted by recommendations 1a, c and d of the Report of the United Nations Secretary General's High-level Panel on Digital Cooperation, and calls made by the UN Broadband Commission and the Internet Governance Forum. However, these messages have not yet been sufficiently translated into concrete action.

In order to address the multiple digital divides, long-lasting measures should address access and use of the Internet. Supply-side factors can include: the availability of relevant infrastructure, spectrum, bandwidth and/or devices; the amount and intensity of competition in the market; appropriate regulatory policies and market forces that affect the ability and cost of supply, such as competition in the market, infrastructure and licensing policies; as well as state-ordered network disruptions. Demand-side factors can include: cost of data and devices; taxation, including both fees on service as well as duties and taxes on equipment and providers; level of education/digital literacy; availability of relevant content/language online; structural and cultural barriers, including discrimination against women and girls; as well as censorship, arbitrary or unlawful surveillance and other privacy-related concerns.

Promoting digital inclusion is of concern to the FOC as it is directly linked to its mandate of protecting and promoting both the exercise of human rights online and supporting an open and interoperable Internet, as affirmed in the FOC's Tallinn Agenda. The Internet and ICTs provide a unique platform to enable individuals to exercise their human rights more fully. Only with meaningful access to the Internet will all individuals be able to reap the economic, social and educational benefits of ICTs and fully exercise their human rights online.

4. Challenges

A. One of the key challenges in ensuring that all relevant stakeholders coherently and systematically engage in promoting digital inclusion and thereby contribute to an open and interoperable Internet is **the need for reliable data and metrics,** as recognized by recommendation 1c of the Report of the United Nations Secretary General's High-Level Panel on Digital Cooperation. First, there is a crucial need for governments to gather better and more consistent data in cooperation with the private sector and institutions responsible for collecting data, disaggregated to provide information across demographic groups for those who face challenges to digital inclusion. Besides cooperating with local statistics offices and government agencies responsible for data gathering, the private sector should be encouraged to share anonymized data within ethical, privacy-protecting frameworks and in accordance with data protection laws.

Collecting disaggregated data at the sub-national level is expensive, a cost many developing countries cannot afford. Donors, including multilateral development banks, should fund this detailed data collection as part of larger investments in ICT and other infrastructure in developing countries. It also means assisting developing countries to use data collection methodologies that measure the degree of exclusion of marginalized groups, and use common criteria to enable identification of groups needing support.

B. Given the complex and broad nature of the digital divides**, it is important that efforts to address inclusion involve all relevant stakeholders.** This vital multi-stakeholder model of governance requires effective partnership between the private and the public sector as well as the private sector and civil society through fora like the Internet Governance Forum.

While governments have an important role to play in promoting digital inclusion, the process of Internet governance should also include active participation by the private sector and civil society. Governments should recognize the important role a competitive private sector and vibrant civil society play in Internet governance. Government should bring relevant actors together and establish conditions that allow enhanced cooperation to take place, including ensuring that policy processes are inclusive, bringing in necessary expertise and input from affected communities.

Additionally, governments should work with the private sector and civil society to create a regulatory environment, which provides for open, interoperable, reliable and secure Internet services that empower users, build trust and foster transparency.

C. It is important to recognize that digital divides often reflect and reinforce existing social and economic inequalities. In supporting digital inclusion, governments should **consider not only access but the online experience itself,** with special attention to novice or non-skilled users of ICTs and/or members of vulnerable or marginalized groups. Challenges include illiteracy, language barriers, social norms that exclude women from using ICTs, wide-spread infringements upon copyright and related intellectual property rights, online fraud, abuse and gender-based violence online, harmful content and disinformation online, surveillance, cybersecurity threats, and the impact of the "gig economy" on workers' rights.

Governments should address such challenges with policies that support enabling environments, such as programs supporting digital literacy as well as inclusive policy processes, and appropriately address the social norms and other barriers that contribute to digital divides.

Efforts by governments to address these negative implications must themselves be consistent with international human rights obligations. Indeed, adopting human rights-based approaches to access is an important enabler of digital inclusion that both encourages open dialogue online while providing safeguards for vulnerable populations.

D. Given **the immense range and number of policies that can potentially affect Internet access**, it is especially important to make focused and systematic efforts to better influence the broad spectrum of policies, regimes, and legislation that can impact digital divides. These efforts have to address supply-side as well as demand-side barriers to digital inclusion. Moreover, these efforts should pay due regard to the underlying obstacles to digital inclusion, including, inter alia, a lack of education and/or digital literacy, poverty, cultural and social barriers and discrimination.

Moreover, an effective approach to Internet policy should also include an impact assessment mechanism that would assess a policy's capacity to further digital inclusion.

5. Call to Action

To address these challenges and to advance the common goal of promoting digital inclusion, the FOC suggests:

- The conduct and support of **good quality, independent research**, on supply and demand-side challenges affecting digital inclusion and digital divides. Research activities should investigate existing and emerging issues related to digital access that may negatively affect digital inclusion by deterring Internet use, such as human rights violations and abuses relating to privacy, online abuse, censorship, surveillance and other cybersecurity methods that limit individuals' ability to exercise their human rights and fundamental freedoms. Governments should also encourage more efforts by the private sector to publish independent, research-based reviews on their data sets, conducted within an ethical, privacyprotective framework.

- **Civil society organizations should be supported in their efforts to address barriers and bottlenecks** to digital access, cybersecurity risks, and on how to develop policy that drives positive outcomes related to the improved access and use of digital technologies. Moreover, all stakeholders should be encouraged to share best practices on issues pertaining to bridging digital divides, especially in support of community networks, and enabling digital inclusion, and governments should play a supportive role in facilitating this.

- **Welcoming contributions, and leadership, by the private sector and civil society** to promote digital inclusion. Encourage the private sector to ensure that resources accrued for the purpose of overcoming digital divides are used transparently for their intended purpose in line with the UN Guiding Principles on Business and Human Rights.

- **Encouraging the availability of free Internet access points in public spaces**, especially in schools and libraries in economically underprivileged communities.

- **Promoting open source** software, open access technologies, open data, and open learning towards enabling meaningful access, as well as supporting the people who develop these resources.

- Enacting digital policies which give **special consideration to those who face particular difficulties** in reaping the benefits of digital inclusion. Governments should build into their programs and policies safeguards to make sure these persons are able to benefit fully in the push for digital inclusion. These may consist of, inter alia, creating safe and accessible spaces, childcare facilities and specially trained support staff.

- Advancing, with the help of public-private partnerships, **digital literacy and other technology training** in trusted and comfortable locations (libraries, community centers, places of worship, schools, recreation centers, senior centers, etc.) which is tailored for different levels of education and specific needs and supported.

- Facilitating, reinforcing, and developing **multi-stakeholder models of Internet governance**, including growing capacity of civil society to participate in fora like the Internet Governance Forum, expanding availability of independent Internet exchange points, ensuring ability of private sector providers to connect and exchange data traffic directly with one another, and similar inclusive models.

- **Addressing underlying causes of digital exclusion** (economic, social, political and cultural contexts) because technical solutions alone will not bridge digital divides; and, support initiatives at intergovernmental spaces that further digital inclusion.

Access is a critical component to furthering digital inclusion but not the only component. Building a digitally inclusive community characterized by access to ICTs and by digital literacy is a multi-faceted process that requires the involvement of both state and non-state actors backed by comprehensive and sustainable policies. These efforts will eventually lead to open and accessible platforms, which allow individuals to benefit from the countless opportunities offered by ICTs and exercise their human rights more fully online.

FOC Joint Statement on Artificial Intelligence and Human Rights

The Freedom Online Coalition (FOC) is a group of 32 countries deeply committed to the promotion and protection of human rights and fundamental freedoms both offline and online. We are committed to working together to support Internet freedom and human rights for individuals worldwide – including the freedoms of expression, association, peaceful assembly, and privacy rights.

The FOC acknowledges that artificial intelligence (AI) systems[1] offer unprecedented opportunities for human development and innovation, with the potential to generate social and economic benefits and help protect and

[1] The OECD defines an AI system as "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of

promote human rights and fundamental freedoms. When developed and used in full respect of human rights, AI systems can complement human endeavours across fields such as public and precision health and environmental science to improve people's lives and support the UN Sustainable Development Goals. States play a critical role in promoting these benefits for all.

As is considered with other digital technologies, AI systems can also be developed or used in ways that pose significant risks to human rights, democracy, and the rule of law. The FOC is particularly concerned by the documented and ongoing use of AI systems for repressive and authoritarian purposes, including through remote biometric identification (RBI) such as facial recognition technology,[2] as well as automated content moderation. Some states use these AI systems, often by leveraging private sector tools, to facilitate and/or mandate arbitrary or unlawful surveillance practices, and censorship practices, that are in violation of international human rights law. The application of AI systems towards repressive and authoritarian purposes can further enable and scale human rights violations and abuses.

The use of RBI and automated content moderation, especially when used by states in an unlawful or arbitrary manner, can threaten the enjoyment of human rights, including the right to equal protection of the law without discrimination and privacy rights. In particular, the use of RBI for repressive and authoritarian purposes threatens the enjoyment of the rights to freedom of religion or belief, freedom of association, peaceful assembly, and liberty of movement. Likewise, the use of automated content moderation for repressive and authoritarian purposes further threatens the enjoyment of the right to freedom of expression, including the freedom to seek, receive and impart information of all kinds, and the freedom to hold opinions without interference. This may result in a chilling effect on the right of peaceful assembly and on freedom of expression in online spaces, as well as undermine the integrity of democratic electoral processes.

The use and deployment of AI systems in ways that violate human rights, and particularly for repressive and authoritarian purposes, threatens online and offline democratic and civic spaces, including political dissent and the important work of journalists and other media workers, human rights defenders, and members of civil society worldwide. This may also further marginalize and oppress persons or groups, such as women and members of ethnic, religious and other minority communities that already face multiple and intersecting forms of discrimination.

As a first step towards the promotion and protection of human rights, states and the private sector should endeavour to promote and increase transparency, traceability, and accountability in the design, development, procurement, and use of AI systems, with appropriate protections for intellectual property. This can help reduce the opacity, inscrutability, and unpredictability of some AI systems and help stakeholders better understand how semi-autonomous AI systems make decisions. The governance, development, and application of AI systems that are grounded in respect for human rights will promote public trust to the benefit of humanity in the long-term.

The FOC reaffirms that states must abide by their obligations under international human rights law to ensure that human rights are fully respected and protected. As also noted in the UN *Guiding Principles on Business and Human Rights*, "States must protect against human rights abuse within their territory and/or jurisdiction by third parties, including business enterprises."[3] We welcome multi-stakeholder attention to this issue in international fora.

Calls to action:

autonomy." OECD Legal Instruments, *Recommendation of the Council on Artificial Intelligence*, May 21, 2019. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

[2] Remote biometric identification (RBI) relies on biometric information (e.g. facial images, iris scans, gait analysis) and can give governments the ability "to ascertain the identity (1) of multiple people, (2) at a distance, (3) in public space, (4) absent notice and consent, and (5) in a continuous and on-going manner." Laura K. Donohue, "Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age." Georgetown Law, 2012. https://scholarship.law.georgetown.edu/facpub/1036/

[3] United Nations, *Guiding Principles on Business and Human Rights*, 2011. https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf

To promote respect for human rights, democracy, and the rule of law in the design, development, procurement, and use of AI systems, the FOC calls on states to work towards the following actions in collaboration with the private sector, civil society, academia, and all other relevant stakeholders:

- States should take action to oppose and refrain from the use of AI systems for repressive and authoritarian purposes, including the targeting of or discrimination against persons and communities in vulnerable and marginalized positions and human rights defenders, in violation of international human rights law.

- States should refrain from arbitrary or unlawful interference in the operations of online platforms, including those using AI systems. States have a responsibility to ensure that any measures affecting online platforms, including counter-terrorism and national security legislation, are consistent with international law, including international human rights law. States should refrain from restrictions on the right to freedom of opinion and expression, including in relation to political dissent and the work of journalists, civil society, and human rights defenders, except when such restrictions are in accordance with international law, particularly international human rights law.

- States should promote international multi-stakeholder engagement in the development of relevant norms, rules, and standards for the development, procurement, use, certification, and governance of AI systems that, at a minimum, are consistent with international human rights law. States should welcome input from a broad and geographically representative group of states and stakeholders.

- States need to ensure the design, development and use of AI systems in the public sector is conducted in accordance with their international human rights obligations. States should respect their commitments and ensure that any interference with human rights is consistent with international law.

- States, and any private sector or civil society actors working with them or on their behalf, should protect human rights when procuring, developing and using AI systems in the public sector, through the adoption of processes such as due diligence and impact assessments, that are made transparent wherever possible. These processes should provide an opportunity for all stakeholders, particularly those who face disproportionate negative impacts, to provide input. AI impact assessments should, at a minimum, consider the risks to human rights posed by the use of AI systems, and be continuously evaluated before deployment and throughout the system's lifecycle to account for unintended and/or unforeseen outcomes with respect to human rights. States need to provide an effective remedy against alleged human rights violations.

- States should encourage the private sector to observe principles and practices of responsible business conduct (RBC) in the use of AI systems throughout their operations and supply and value chains, in a consistent manner and across all contexts. By incorporating RBC, companies are better equipped to manage risks, identify and resolve issues proactively, and adapt operations accordingly for long-term success. RBC activities of both states and the private sector should be in line with international frameworks such as the UN *Guiding Principles on Business and Human Rights* and the OECD *Guidelines for Multinational Enterprises*.[4]

- States should consider how domestic legislation, regulation and policies can identify, prevent, and mitigate risks to human rights posed by the design, development and use of AI systems, and take action where appropriate. These may include national AI and data strategies, human rights codes, privacy laws, data protection measures, responsible business practices, and other measures that may

[4] OECD, *Guidelines for Multinational Enterprises,* 2011. http://mneguidelines.oecd.org/guidelines/

protect the interests of persons or groups facing multiple and intersecting forms of discrimination. National measures should take into consideration such guidance provided by human rights treaty bodies and international initiatives, such as human-centered values identified in the OECD *Recommendation of the Council on Artificial Intelligence*,[5] which was also endorsed by the G20 AI Principles.[6] States should promote the meaningful inclusion of persons or groups who can be disproportionately and negatively impacted, as well as civil society and academia, in determining if and how AI systems should be used in different contexts (weighing potential benefits against potential human rights impacts and developing adequate safeguards).

- States should promote, and where appropriate, support efforts by the private sector, civil society, and all other relevant stakeholders to increase transparency and accountability related to the use of AI systems, including through approaches that strongly encourage the sharing of information between stakeholders, on topics such as the following:
    - user privacy, including the use of user data to refine AI systems, the sharing of data collected through AI systems with third parties, and if reasonable, how to opt-out of the collection, sharing, or use of user-generated data
    - the automated moderation of user generated content including, but not limited to, the removal, downranking, flagging, and demonetization of content
    - recourse or appeal mechanisms, when content is removed as the result of an automated decision
    - oversight mechanisms, such as human monitoring for potential human rights impacts

- States, as well as the private sector, should work towards increased transparency, which could include providing access to appropriate data and information for the benefit of civil society and academia, while safeguarding privacy and intellectual property, in order to facilitate collaborative and independent research into AI systems and their potential impacts on human rights, such as identifying, preventing, and mitigating bias in the development and use of AI systems.

- States should foster education about AI systems and possible impacts on human rights among the public and stakeholders, including product developers and policy-makers. States should work to promote access to basic knowledge of AI systems for all.

---

[5] OECD, *Recommendation of the Council on Artificial Intelligence*, May 21, 2019. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

[6] "G20 Ministerial Statement on Trade and Digital Economy - Annex, G20 AI Principles," June 9, 2019. https://www.mofa.go.jp/files/000486596.pdf