Ottawa, March 11th, 2022
Secretariat
Office of the United Nations High Commissioner for Human Rights (OHCHR)
Palais Wilson
52, rue des Pâquis
CH-1201 Geneva, Switzerland
OHCHR-bhr@un.org

Subject: The Freedom Online Coalition's submission to the OHCHR regarding the practical application of the UNGPs in the global technology sector (A/HRC/RES/47/23)

As chair of the Freedom Online Coalition (FOC) for 2022, Canada is pleased to have the opportunity to share the work the FOC has undertaken to promote the implementation of the UN Guiding Principles on Business and Human Rights (UNGPs) in the global technology sector in response to the OHCHR's call for input pursuant to Human Rights Council resolution 47/23 on "New and emerging digital technologies and human rights". Our response is focused on the first pillar of the UNGPs, namely the States' existing obligations to respect, protect and fulfil human rights and fundamental freedoms (duty to protect).

Composed of 34 governments committed to protecting human rights in online and digital contexts, the FOC is committed to and plays a key role in ensuring member States and other States fulfil their duty to protect when interacting with the global technology sector. In this year's program of action, the FOC has committed to promote the UNGPs through, among others, collaboration with the private sector, civil society, and other stakeholders. This commitment fits within the FOC's broader priorities during Canada's chairship which consist in affirming and shaping global norms, promoting multi-stakeholder engagement, and ramping up advocacy, communication, and outreach. As an international forum, the FOC advances the UNGPs in the global technology sector mainly through norm development and diplomatic coordination.

Norm Development

The first way in which the FOC promotes the practical application of the State duty to protect to the global technology sector is through norm development. The FOC has established an extensive set of positions articulating how human rights online can be upheld and expanded by States and the private sector in a range of areas, including countering disinformation, enhancing cybersecurity, developing trustworthy artificial intelligence (AI) and expanding digital inclusion.

The FOC communicates its positions through "joint statements" which are carefully negotiated and reflect the input of the FOC's multi-stakeholder Advisory Network. FOC joint statements regularly call upon technology companies to comply with the UNGPs. For example, the Joint Statement on Artificial Intelligence and Human Rights released in 2020 called upon States to encourage the private sector to observe the principles and practices of responsible business conduct (RBC) in the use of AI systems throughout their operations and supply and value chains in line with international frameworks such as the UNGPs and the OECD Guidelines for Multinational Enterprises. In the FOC Joint Statement on Restrictive Data Localisation Laws released in 2015, the Coalition invited companies, when required by laws or regulations to store data locally, to "conduct appropriate human rights due diligence consistent with the UN Guiding Principles on Business and Human Rights."

Moreover, joint statements often include calls for action addressed directly to technology companies. For example, in the Joint Statement on Spread of Disinformation Online released in 2020, the FOC urged social media platforms and the private sector to address disinformation in compliance with the UNGPs, increase transparency, provide users with appeal processes, use independent and impartial fact-checking services, take measures to strengthen the provision of independent news, support research, and more.

Diplomatic Coordination

A second way in which the FOC promotes the practical application of the State duty to protect in a digital world is through diplomatic coordination. Owing to its established network of contact points across capitals and international forums and its multi-stakeholder Advisory Network, the FOC has enormous potential for coordination among member States and stakeholders. FOC member States build policy coherence with respect to the UNGP's State duty to protect by sharing information and best practices in a rapidly evolving digital environment.

The FOC also maintains strong ties with the global technology sector. In March 2021, the FOC launched the Silicon Valley Working Group with the aim to build new forms of cooperation between the FOC and the global technology sector whose products or services potentially impact human rights, many of which are headquartered in Silicon Valley and the US West. This diplomatic network allows for the FOC to raise awareness about the UNGPs and improve information flows and transparency between the global technology sector in Silicon Valley and home governments as well as the multilateral community. Moreover, the FOC Advisory Network comprises representation from technology companies including Facebook and Microsoft. The FOC member States engage regularly with the network which provides comments on draft statements, advice to governments and organises multistakeholder collaboration around FOC activities. More and more often, the Advisory Network serves as an accountability mechanism for States to respect their commitments to UNGPs towards technology companies.

The role the FOC plays in ensuring member States and other States fulfil their duty to protect when interacting with the global technology sector can be illustrated through its work on disinformation and artificial intelligence.

Disinformation

The FOC addressed the State duty to protect under the UNGPs in its Joint Statement on Spread of Disinformation Online released in 2021 (see annex) and, recently, in Canada's Declaration as the Chair of the FOC on State-sponsored Disinformation in Ukraine released in 2022.[1] Disinformation, whether state- or business-sponsored, can undermine many human rights including – freedom of opinion and expression, the right to take part in the conduct of public affairs and to vote in elections, protection against discrimination, protection of honour and reputation, the right to health, and the right to education. According to UNGPs' State duty to protect, States should take all appropriate steps to prevent, investigate, punish, and redress human rights violations caused by businesses, including technology companies. Conversely, it is imperative that States do not use their obligations to protect against human rights harms as cover to shape tech companies' practices, products and services in ways that cause or contribute to human rights violations. In other words, States should not mandate technology companies to violate human rights.

This is why FOC declarations and statements on state-sponsored disinformation call upon governments not to unduly restrict, moderate or manipulate online content or disrupt networks to deny users access to information, contrary to their international obligations and often under vague justifications of "security", "public order", or the false pretention of combatting "fake news". This call has been repeated in various joint statements over the years.[2] [3] Canada's Declaration as the Chair of the FOC on State-sponsored Disinformation in Ukraine reflects the enhanced importance of this duty in the context of the State-business nexus of state-owned or state-controlled media corporations as well as during armed conflicts where risks of disinformation are higher.

States' duty to protect also include the obligation to adopt a "smart-mix" of measures (i.e., policies, laws, and regulations) to foster businesses' respect for human rights, including in the global technology sector. These measures should enable, encourage, guide, and sometimes mandate technology companies to respect

[1] The declaration has been endorsed by the following FOC member States: Australia, Austria, the Czech Republic, Denmark, Estonia, Finland, Germany, Ireland, Italy, Latvia, Lithuania, Luxembourg, the Netherlands, Norway, Poland, Sweden, the United Kingdom, and the United States.

[2] *See* Joint Statement on Defending Civic Space Online (May 2019); Joint Statement on Internet Censorship (May 2018); Joint Statement and Accompanying Good Practices for Government on State-Sponsored Network Disruptions (March 2017); Joint Statement on Cross-Border Attacks on Freedom of Expression Online (March 2016).

[3] The FOC has denounced other State actions directed towards technology companies that stood in direct contravention with their duty to protect in previous joint statements. Condemned State actions include, for example, compelling facial recognition and cybersecurity technology suppliers to cooperate with their security and intelligence agencies without any democratic or independent check or balances on these authorities (Joint Statement on the Human Rights Impacts o of Cybersecurity Laws, Practices and Policies (February 2020); leveraging technology companies to attack freedom of expression abroad (Joint Statement on Cross-Broder Attacks on Freedom of Expression Online (March 2016)); and using privacy and security considerations as a pretext to force Internet companies and service providers to store user data on servers physically located within their domestic borders (Joint Statement on Restrictive Data Localization Laws (2015)).

human rights. Proper human rights guidance includes sharing best practices and encouraging technology companies to share information on how they address their human rights impacts. In the case of disinformation, the FOC has established several guidelines for platforms that States should adopt to foster the platforms' compliance with the UNGPs and international human rights law when countering disinformation:

- Address disinformation in a manner that is guided by respect for human rights and the UN Guiding Principles on Business and Human Rights.
- Increase transparency into the factors 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 identify 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 building appropriate mechanisms for reporting, designed in a multi-stakeholder process and without compromising effectiveness or trade secrets.
- Promote users' access to meaningful and timely appeal processes to any decisions taken in regard to the removal of accounts or content.
- Respect the rule of law across the societies in which they operate, while ensuring not to contribute to violations or abuses of human rights.
- Use independent and impartial fact-checking 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.

(Joint Statement on Spread of Disinformation Online (November 2020))

Artificial Intelligence

Another example of the role the FOC plays with respect to the UNGPs' State duty to protect in the global technology sector is in the context of the development, deployment, and use of artificial intelligence (AI) systems.

One issue of particular importance to FOC members has been the documented and ongoing use of AI systems for repressive and authoritarian purposes, including through remote biometric identification such as facial recognition technology, 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 FOC condemns these State actions in its Joint Statement on Artificial Intelligence and Human Rights released in 2020 (see annex).

In the joint statement, the FOC has also mentioned several measures that States should adopt to guide technology companies involved in the development of AI systems to respect human rights. First, States – as well as any private sector or civil society actors working with them or on their behalf – should adopt processes such as due diligence and impact assessments when procuring, developing, and using AI systems in the public sector. These assessments should be informed by inputs from stakeholders, particularly those who face disproportionate negative impacts, and made transparent. Impact assessments should minimally 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.

Second, 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. Topics on which information sharing is encouraged are:

- 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

(Joint Statement on Artificial Intelligence and Human Rights (November 2020)

Conclusion

The digital technologies and Internet fields are evolving rapidly and pose unprecedented risks to human rights in terms of both nature and scale. Being at the forefront of issues at the intersection of digital technologies, Internet, and human rights, the FOC serves as an increasingly essential forum for States and technology companies to protect human rights online and flesh out the UNGPs in a digital world.

Despite the progress made through the FOC, some challenges remain, especially with respect to our understanding of how international human rights law can address the rapidly evolving and unprecedented risks posed by digital technologies. This is why Canada, as chair of the FOC for 2022, fully supports the work of B-Tech and is currently seeking to organize a workshop on the margins of HRC 51 to deepen this understanding. The workshop will focus on the applicability of the obligation of non-discrimination under international law to the risks posed by digital technologies, including artificial intelligence.

Annex – FOC Joint Statement on Spread of Disinformation Online

November 2020

FOC Joint Statement on Spread of Disinformation Online

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[3], 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

[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 ICCPR]; protection of honour and reputation [Art. 17 ICCPR]; the right to health [Art. 12 ICESCR]; the right to education [Art. 13 ICESCR].
[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 concern about shrinking civic and democratic spaces online as a result of state-sponsored obstruction of free expression, peaceful assembly, and free association.

disinformation campaigns by state and state-sponsored actors can also be used as part of hybrid influence campaigns[5] 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 information. For example, the use of algorithms to promote certain content can lead to the amplification and prioritization 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.

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.

[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".

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. https://freedomonlinecoalition.com/document/foc-jointstatement-on-digital-inclusion/

The FOC urges social media platforms 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 factors 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 identify 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 building appropriate mechanisms for reporting, designed in a multi-stakeholder process and without compromising effectiveness or trade secrets.

- Promote users' access to meaningful and timely appeal processes to any decisions taken in regard to the removal of accounts or content.

- Respect the rule of law across the societies in which they operate, while ensuring not to contribute to violations or abuses of human rights.

- Use independent and impartial fact-checking 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.

[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 Principles on Business and Human Rights, 2011. https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf

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 ensuring 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.

Annex – FOC Joint Statement on Artificial Intelligence and Human Rights

November 2020

FOC Joint Statement on Artificial Intelligence and Human Rights

The issue

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 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

[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 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/

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.

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

Call to action

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]

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

- 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 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