Global Digital Compact

Global Partners Digital submission
April 2023

About Global Partners Digital

Global Partners Digital is a social purpose company dedicated to fostering a digital environment underpinned by human rights.

Introduction

We welcome the opportunity to provide written input to the Global Digital Compact consultations. We also submitted this input via the online form for the written consultation, now available via an interactive platform on the Global Digital Compact website.[1] In this input, we provide our input to components 2-6 of the consultation:

- 2. Avoid internet fragmentation
- 3. Protect data
- 4. Apply human rights online
- 5. Accountability for discrimination and misleading content
- 6. Regulation of artificial intelligence

As requested, we have organised our views and inputs, along the following two aspects:

1. Core principles that all governments, companies, civil society organisations and other stakeholders should adhere to; and
2. Key commitments, pledges, or actions that in your view should be taken by different stakeholders – governments, private sector, civil society, etc

Response

Avoid internet fragmentation

a) Core Principles

[1] https://www.un.org/techenvoy/global-digital-compact/submissions

- The work of the UN and all its relevant agencies should continue to be anchored in the values and obligations of the UN Charter, Universal Declaration of Human Rights, and the UN Guiding Principles on Business and Human Rights.
- All stakeholders should promote the open, distributed and interconnected nature of the Internet so that it can continue to be a globally connected, stable, unfragmented, scalable, accessible and open network of networks.
- All stakeholders should protect and promote the global free flow of information, ensuring that the economic and social benefits of the Internet and related digital technologies continue to flourish and support the Sustainable Development Goals.
- Laws and policies should not place barriers to global connectivity and should take into account the architecture of the internet.
- Stakeholders should cooperate to promote security and increase trust in the Internet. The implementation of international best practices is essential in addressing security threats and reducing vulnerabilities, which should be operationalised through cooperation by different stakeholders.
- Access to the Internet plays a vital role in the full realisation of human development and facilitates the enjoyment of a number of human rights, as well as other benefits. Meaningful connectivity (regular, affordable, and secure access) to the internet and device accessibility should be available to all.
- All stakeholders should commit to preserving and strengthening the multistakeholder model, ensuring that UN policymaking processes are more diverse, equitable, and inclusive and that existing fora tasked with Internet governance challenges, such as the Internet Governance Forum, have appropriate human resources and funding.

b) Key Commitment/Pledges/Actions

States

- States should protect the Internet's key characteristics (accessible, interoperable, decentralised, global and neutral) and not implement policies or actions which restrict the free flow of information in contravention of international human rights law standards.
- States should align legislation which may impact the free flow of information online (e.g. data protection laws) with international human rights standards.
- States should not implement measures that impede the interoperability of the internet or which would restrict access to certain types of data or information.
- States should not seek to influence technical protocols and standards or their implementation in a way that would impede the free flow of information globally or otherwise act in ways that do not promote and encourage respect for human rights.

- States should ensure that individuals can access the Internet easily and regularly through affordable and secure broadband. Access must be meaningful and safe for all, enabled by digital literacy and trust. Access that contributes to the well-being of societies must have human rights at its centre.
- States should take action to regulate business practices that threaten a global and interoperable Internet, such as walled gardens.
- States should promote an open Internet in relevant multilateral and multi-stakeholder forums, and ensure that processes are open, inclusive, consensus-driven and transparent. This includes ensuring that stakeholders from the global South and other typically under-represented groups in global public policymaking can fully participate in decision-making processes and providing adequate notice and funding and accessible accreditation systems.

Companies

- Companies should adopt a principled approach grounded in the *United Nations Guiding Principles on Business and Human Rights* (UNGPs) for ensuring that their practices do not restrict the free flow of information globally. Respect for human rights should be operationalised as part of how they do business through human rights due diligence, by critically assessing government demands or regulations which restrict the free flow of information.
- Companies should work together to develop and implement industry norms and standards which enable an open and interoperable Internet.

3. Protect data

a) Core Principles

- International human rights law should act as the basis for protecting personal data. It provides a clear and universal framework for the promotion and protection of the right to privacy, which has been interpreted to cover the collection, processing, sharing and use of personal data.
- The collection, processing, sharing and use of personal data should be subject to personal data protection regulation that is in line with international human rights law standards. This includes ensuring that individuals are able to provide their explicit and informed consent to the collection, processing and storage of their personal data or its re-use., and that individuals have access to remedy in the case of their data being misused, leaked or stored without their consent.
- No one shall be subjected to arbitrary interference with the right to privacy, and any restriction on this right must be consistent with the principles of legality, necessity and proportionality.

- In practice, this also means that any surveillance, interception or collection of individuals' data should be fair, lawful, transparent, and subject to independent oversight and that affected individuals should be provided with access to remedies.
- Effective personal data protection frameworks should also tackle micro-targeting and commercial surveillance based on user data.
- Effective personal data protection frameworks should prevent the use of data in a discriminatory way and provide effective remedies in the case of users' data being used for disfavoring them based on their race, ethnicity, sex, gender identity, sexual orientation, religion, age, national origin, medical conditions, disability, genetic information, or any other characteristic protected by law.
- Personal data protection efforts should also support and encourage the use of effective cybersecurity measures for safeguarding personal information from hacking or cyberattacks, including measures to protect strong encryption.
- There should be a coordinated and multi-stakeholder approach to the protection of critical infrastructure, which is key for the protection of personal data and in responding to incidents that may pose risks to individuals' right to privacy.
- Cross-border data sharing agreements should not be used to circumvent existing protections for privacy and personal data protection at the national level and should contain relevant safeguards to prevent risks to human rights and especially the right to privacy.

b) Key Commitment/Pledges/Actions

States

- States should review existing procedures, practices, and legislation relating to the protection of personal data to ensure that they comply with international law. This includes practices and legislation regarding the surveillance or interception of communications as well as laws governing the collection and processing of personal data.
- States should adopt comprehensive frameworks on data protection that are aligned with international standards and best practice such as Convention 108+ and the OECD Privacy Guidelines, which include requirements for independent oversight, grievance mechanisms and access to remedy. These frameworks should also address issues of micro-targeting and commercial surveillance.
- States should ensure that such frameworks introduce accountability for private actors undertaking practices that are inconsistent with the right to privacy and protection of personal data.
- States should not introduce legislation which undermines privacy-enhancing and privacy-protecting technologies like encryption.

- States should not encourage, incentivise or mandate the use of invasive technologies – such as facial recognition or age verification software or biometric tools – by any public or private actor. Where such tools are deployed, states should implement prior human rights impact assessment and rigorous safeguards around how biometric data is used, stored and processed.
- States should ensure that personal data-driven technologies deployed as part of their policies are subject to prior human rights impact assessment, subject to democratic scrutiny in their adoption, and ongoing independent oversight to avoid discriminatory impact on the population and other adverse human rights impacts.

Companies

- Companies should update their terms of service and privacy policies to align with international standards and best practices such as Convention 108+ and the OECD Privacy Guidelines.
- Companies should extend privacy by design and privacy-enhancing technologies, including encryption, as a means of safeguarding individuals' communications and personal information.
- Companies which collect personal data should ensure that they have robust infrastructure, policies and safeguards in place to prevent data breaches and to inform users of any such data breaches when they occur.

Civil society

- Civil society should advocate for comprehensive personal data protection and privacy legislation, as well as their implementation and enforcement.
- Civil society should conduct research and monitor how personal data may be misused by public or private actors and the ways they may impact particular communities, including marginalised groups, human rights defenders and women.

4. Apply human rights online

a) Core Principles

- Human rights (as set out in the Universal Declaration of Human Rights and enshrined in other relevant international human rights treaties) apply online. Individuals enjoy the same human rights online as they enjoy offline.
- States have obligations under international human rights law to respect, protect and fulfil human rights online. Companies have a responsibility to respect human rights online as set out in the UNGP.
- The Internet is a key enabler for the exercise and enjoyment of human rights, both

civil and political rights and economic, social and cultural rights.

- The existence and expansion of affordable, reliable and secure access to the Internet facilitates the full enjoyment of human rights.
- To enable human rights the Internet has to be safe for all individuals without fear of persecution, discrimination or harassment.
- Technical solutions to protect the confidentiality of digital communications, such as encryption and anonymity, are critical for the enjoyment of all human rights offline and online. This is because the right to privacy is a gateway right, allowing individuals to exercise other rights.
- Internet shutdowns have an overwhelmingly negative impact on the enjoyment of human rights online and offline. Shutdowns restrict individuals' rights to freedom of expression and access to information, peaceful assembly, and the right to vote, as well as impacting the fulfilment of economic, social, and cultural rights.

b) Key Commitment/Pledges/Actions

States

- States should develop Internet-related laws and policies in a way that is underpinned by human rights and developed in an open, inclusive and transparent manner.
- States should repeal any law that unduly restricts freedom of expression or privacy in the digital environment. Restrictions on freedom of expression and privacy are only permissible when they are provided by law, are in pursuance of a legitimate aim, and are necessary and proportionate.
- States should ensure that individuals have access to effective remedies for human rights violations relating to the use or access of the Internet, in accordance with their international obligations.
- States should take extra steps to protect the rights of vulnerable and marginalised groups in the online environment, and should consult with such groups whenever developing internet-related laws or policies to ensure that such laws or policies do not disproportionately impact or restrict the rights of such groups.
- States should commit themselves to bridging digital divides, including the gender digital divide, and to expand Internet access in order to promote the full enjoyment of human rights.
- States should advance capacity-building and digital literacy initiatives.
- States should implement Human Rights National Action Plans to address the responsibility of internet services and products companies to ensure the exercise of human rights in line with the UNGP.

Companies

- Companies should embed human rights principles in the design, development, deployment and monitoring of any internet-related tool or product. This includes taking steps to identify and mitigate human rights risks posed by their services, consulting with affected stakeholders, and ensuring that users have access to remedy for any rights violations that may occur according to UNGP.
- Companies should continue to provide tools to ensure safety online, including through encryption or other means of providing protection for individuals online.
- Companies should take extra steps to identify and mitigate risks that their products and services may pose to enable human rights through constant human rights due diligence, and engage with concrete commitments in Human Rights National Action Plans to address their responsibilities according to the UNGP.

Civil Society

- Civil society organisations should work to hold governments and companies to account for their adherence to relevant international obligations and responsibilities, as well as advocating for rights-respecting approaches to Internet regulation at the national, regional and global levels.

5. Accountability for discrimination and misleading content

a) Core Principles

- States have obligations under international human rights law to respect, protect and fulfil human rights online. Discriminatory and misleading online content may pose a range of risks to individuals' human rights, including by limiting access to reliable and accurate information, to express oneself freely online without fear of being targeted, and to health, life and bodily integrity.
- Companies that provide platform services have a responsibility to respect human rights and should be accountable for the human rights impacts of their services and products according to international human rights law, in particular under the framework of the UN Guiding Principles on Business and Human Rights.
- International human rights law should be the basis for providing accountability for discrimination and misleading content as it provides clear guidance on what restrictions on speech are compatible with the right to freedom of expression:
    - Restrictions on discriminatory and misleading online content should be provided for in law in a manner which is sufficiently clear for an individual to know what speech or conduct is prohibited.
    - Restrictions on discriminatory and misleading online content should pursue legitimate aims as set out under Article 19(3) of the ICCPR, including to

protect the rights or reputations of others, for the protection of national security or of public order, public health or public morals. Restrictions should also be proportionate and necessary – i.e. the least restrictive measures possible to achieve the stated aim.

- Discriminatory content which is considered advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence must be prohibited under international human rights law (ICCPR Article 20).
- If individuals are to be held accountable or liable for sharing discriminatory and misleading online content, such content must be clearly illegal and liability should be tied to the individual's provable intent to cause harm by sharing such content. Any sanctions should be proportionate to the actual harm caused by the content in question, and individuals should never be held liable for disseminating content which they did not know to be misleading.

b) Key Commitment/Pledges/Actions

States

- States should design responses to misleading and discriminatory online content which are consistent with international human rights law; any restrictions on such content should be clearly formulated in law, in pursuit of a legitimate aim and necessary and proportionate to achieve the stated aim.
- States should ensure that individuals whose speech is restricted on these grounds can appeal such determinations and that determinations of what content falls in scope are made by an independent judicial body.
- States should design responses to misleading and discriminatory online content in an inclusive, transparent and multi-stakeholder fashion.
- States should ensure that internet regulations do not mandate or incentivise online platforms to remove or restrict misleading or discriminatory content in a manner which is inconsistent with international human rights law.
- States should take steps to tackle the root causes of discriminatory and misleading online content, including poor media literacy, misogyny, racism, homophobia and harmful conspiracy theories, for example through intervention programs, peer support networks, digital literacy education and supporting journalists.

Companies

- Companies should implement human rights due diligence mechanisms to address the risks posed by discriminatory or misleading content shared or amplified on their platforms. Particular care should be given to the assessment of algorithms used for engagement and the way in which they disproportionately impact the exposure of

marginalised and vulnerable groups to discriminatory or misleading content.

- Companies should develop clear and transparent policies on discriminatory or misleading content shared on their platforms in consultation with a wide range of stakeholders, particularly marginalised users.
- Companies should ensure that users can report discriminatory or misleading content on their platforms which poses harm, and explain clearly any decisions to remove or not remove such content to the affected users and give them means to appeal such decisions with a specific view to make those mechanisms accessible and usable to marginalised and vulnerable groups.
- Companies should provide regulators and researchers with access to relevant data on the spread and impact of misleading or discriminatory content on their platforms in order to encourage more effective, evidence-based and targeted responses.

Civil society

- Civil society should conduct research on the human rights impacts of misleading and discriminatory online content, particularly on marginalised or vulnerable groups.
- Civil society should advocate for accountability frameworks that are underpinned by international human rights law, and document and report on instances where legal or policy responses to misleading and discriminatory online content result in human rights violations.

6. Regulation of artificial intelligence

a) Core Principles

- The regulation of AI should be firmly rooted within the existing international human rights framework and should not undermine or seek to replace existing human rights standards.
- The international human rights framework and the specific rights guaranteed under it –including the rights to life, privacy, freedom of expression, association, assembly, freedom of movement, non-discrimination and effective remedy – apply to the regulation of artificial intelligence (AI).

b) Key Commitment/Pledges/Actions

States

- States should develop regulation which identifies and mitigates the various means in which AI may pose risks to human rights, including through their own use of AI systems as well as by other actors. State deployment of AI which interferes with the

exercise of human rights is only permitted when the interference is provided for by law, pursues a legitimate aim, is proportionate and is no more than necessary to achieve that aim.

- States should ensure the regulation of AI should take a human rights and risk-based approach which focuses on mitigating potential harms whilst promoting the development and use of AI systems that are beneficial for the enjoyment of human rights.
- States should ensure the regulation of AI should apply to the design, development, application and review of AI systems, or in other words, to all stages of the AI life cycle, particularly when its use has a potential impact on human rights.
- States should ensure the regulation of AI must apply to all relevant actors, including public and private entities, and establish legal obligations where appropriate. This should involve requirements to identify, analyse and evaluate the human rights risks of AI systems.
- States should ensure the regulation of AI must provide effective safeguards, such as redress mechanisms (individual and collective) for those negatively impacted by AI systems. This requires that individuals are informed when an AI system makes a decision which may impact their rights and provides accessibility and explainability for the individual to effectively challenge decisions.
- States should ensure the regulation of AI should include specific provisions which mitigate risks of bias and discrimination. AI must not be deployed in a discriminatory manner.
- States should ensure the regulation of AI should involve prohibitions of certain AI systems when they pose unacceptable risks to human rights that cannot be sufficiently mitigated.
- The regulation of AI should be underpinned by principles of accountability and robust transparency, which are reflected in the Sustainable Development Goals and the UNGPs. This includes accountability mechanisms throughout the AI life cycle by ensuring: human rights impact assessments, algorithmic transparency, auditability and explainability, appropriate oversight procedures, and remedy and enforcement powers for regulators.
- States should apply inclusive approaches and foster meaningful participation in decision-making about AI deployment by ensuring diversity and broad participation in the development of AI regulation and policy implementation.
- States should develop or update personal data protection and anti-discrimination frameworks to respond to the risks to human rights posed by AI.

Companies

- Companies should conduct widespread and systematic human rights due diligence and human rights impact assessments to adequately assess the actual and

potential systemic and specific impacts of AI systems according to UNGPs.

- Companies should ensure that the findings of their assessments are fully integrated into corporate practice through mitigation efforts and remedial actions. These findings should also be made publicly available and on a periodic basis to promote transparency.

Civil Society

- Civil society should advocate for the development and implementation of AI regulation and policies through a multi-stakeholder approach. This should include those representing groups that are likely to be most adversely affected by AI technologies.