Joint Civil Society Input

Pact for the Future

List of signatories: **Global Partners Digital, Access Now, European Center for Not-for-Profit Law (ECNL), Derechos Digitales - América Latina, Association for Progressive Communications**

Chapeau

- The Pact should reaffirm the human rights and fundamental freedoms enshrined in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the International Covenant on Economic, Social, and Cultural Rights and other relevant human rights instruments. It should recognise that the effective implementation of the international human rights law framework is a necessary precondition to ensure the achievement of the Agenda 2023, and that adherence to both is necessary to ensure the realisation of an open, free and secure digital future for all.

- The Pact should include a clear recognition of a state's obligations under international human rights and humanitarian law and the responsibilities of companies under the UN Guiding Principles on Business and Human Rights (UNGPs). This includes the responsibility to foster respect for human rights online and offline in the context of new and emerging digital technologies and human rights due diligence processes.

- The Pact should recognise the existing structural asymmetries and inequalities that underlie the global digital economy, and ensure that measures aim to overcome existing North-South disparities in the exploitation and the benefits of that economy.

- The Pact should encompass an intersectional gender perspective that recognizes and takes into consideration the different impact that digital technologies have on women, girls and people of diverse genders and sexualities.

- The Pact should reaffirm commitments to openness, inclusivity and transparency as key principles for all stages of the implementation and review of the Pact. This should include the inclusion and integration of all perspectives, particularly those subject to discrimination or other forms of marginalization.

- The Pact should ensure holistic integration of digital technologies into all of its chapters and this integration should be reflected in the diversity of stakeholder participation, institutional arrangements and the mechanisms to implement the actions it proposes.

Chapter II. International peace and security

- The Pact should reiterate that international law, including the UN Charter, international humanitarian law and the international human rights law apply to the maintenance of international peace and security.

- The Pact should reaffirm adherence to the universally agreed upon framework of responsible state behavior in cyberspace and its possible future elaboration, where appropriate. To guarantee the effective implementation of the framework in a human-centric manner, the Pact should support and complement the establishment and assessment of a Cyber Programme of Action, ensuring the meaningful participation of all stakeholders in its design, establishment and functioning. It should also reflect ongoing trends of different types of cyber operations threatening peace and security, and the targets of attacks; advance principles-based cyber capacity building in alignment with the Agenda 2030; and build common understanding to ensure the ongoing protective value of international law.

- States should recognize the right to privacy as a universal, indivisible, interdependent human right that applies across borders and media. Recognising that the right to privacy is intrinsically linked to the effective protection of personal data, states should commit to ensuring that personal data protection efforts support and encourage the use of effective cybersecurity measures for safeguarding 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. This should involve transparency and publicity in data incident management.

- States should not introduce legislation which undermines privacy-enhancing and privacy-protecting technologies like encryption. Companies should extend human rights by design and privacy-enhancing technologies as a means of safeguarding individuals' communications and personal information, as well as online safety.

- States should refrain from spreading online content in violation of international law, for example, when it reaches the threshold of a prohibited intervention under the UN Charter, and simultaneously design responses to harmful and discriminatory online content which do not mandate or incentivize online platforms to remove or restrict such content in a manner which is inconsistent with international law. As required under 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 design responses in an open, inclusive and transparent fashion.

- States should implement an immediate moratorium on the export, sale, transfer, use, and servicing of targeted digital surveillance technologies, until rigorous human rights safeguards are in place, and ban said technology and its vendors where they facilitate or enable human rights abuses.

- States should effectively regulate and oversee the activities of private military and security companies, including where they provide cyberservices and operate in the conduct of hostilities, in conflict and in non-conflict settings.

Chapter III. Science, technology and innovation and digital cooperation

- States should support people's right to shape and use digital technologies to meet their specific needs and realities, with the aim of bolstering connectivity, addressing digital divides and supporting the Sustainable Development Goals. This includes supporting unconnected communities and groups to build technical communications infrastructure which provides meaningful access to the Internet outside of existing models, such as through community networks and smaller-sized cooperative operators.

- All stakeholders should commit to promoting and protecting 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. 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 refrain from and prevent the development of standards that facilitate human rights violations and abuses when participating in standard-setting processes.

- International human rights law should serve as the basis for the development of all regulatory frameworks for science, technology, and digital cooperation. These frameworks, including those relating to new and emerging technologies, should be developed in an open, inclusive and transparent manner and foster meaningful participation in decision-making and governance.

- The Pact should encourage states to adopt comprehensive frameworks on data protection that are aligned with international standards and best practice, such as Convention 108+, which include requirements for consent, independent oversight, grievance mechanisms and access to remedy. These frameworks should address issues of micro-targeting and commercial surveillance, as well as providing safeguards against the processing or use of data which disfavors individuals based on any protected characteristic.

- Policy approaches on new and emerging forms of digital technologies, such as artificial intelligence (AI) systems, should be firmly rooted within the existing

international human rights framework and should not undermine or seek to replace existing protections. They should also be underpinned by robust transparency and accountability mechanisms throughout the AI life cycle, such as through human rights impact assessments, stakeholder engagement, algorithmic transparency, auditability and explainability, appropriate oversight procedures, and redress mechanisms (individual and collective) and enforcement powers for regulators.

- The regulation of new and emerging digital technologies, such as AI systems, should take a human rights-based approach which focuses on mitigating potential harms whilst promoting their potential benefits for the enjoyment of human rights. It should apply to all stages of the AI life cycle, and must apply to all relevant actors, including public and private entities.

- The regulation of new and emerging technologies, such as AI systems, should not make exceptions or exclude the use of technologies in the contexts in which they arguably pose the greatest threats to human rights, including but not limited to immigration, national security, counter-terrorism, or intelligence, and should not exclude law enforcement and state agencies from their purview.

- States should ensure the regulation of new and emerging technologies, such as AI systems, include prohibitions on the use of technologies or specific applications when they pose unacceptable risks to human rights that cannot be sufficiently mitigated. These should include, at minimum, AI systems using biometrics to identify, categorize or infer sexual orientation, gender, protected characteristics or the emotions of individuals, in particular if they can lead to mass surveillance; or AI systems used for social scoring, among others.

Chapter V. Transforming global governance

- All stakeholders should commit to preserving and strengthening the multistakeholder model, ensuring that UN policymaking processes are more diverse, equitable, accessible, and inclusive and that existing fora tasked with Internet governance challenges, such as the Internet Governance Forum, have appropriate human resources and funding.

- Connections between existing forums, including the IGF, should be prioritized. The IGF is designed as an open and inclusive forum and should not be replaced or encroached upon by another forum. Any new bodies/fora created for the governance of new and emerging digital technologies should reflect a multistakeholder approach, one that involves civil society and other actors in a meaningful way. This should include those representing groups that are likely to be most adversely affected by such technologies.

- States should promote an open and secure Internet in relevant multilateral and multistakeholder forums, and ensure that processes are open, inclusive, accessible, consensus-driven, and transparent. This includes ensuring that stakeholders from the Global Majority and other under-represented groups in global public policymaking can fully participate in decision-making processes and providing adequate notice and funding and accessible accreditation systems. This does not mean that remote participation suffices as a meaningful way to engage in hybrid or in-person events, but that a multitude of robust participation options, with travel and visa support, should be provided. Any state hosting a forum should undergo human rights due diligence, and fora should strive to meet in locations accessible to a diverse set of stakeholders, in environments characterized by the rule of law and protection for the freedoms of association, peaceful assembly, and expression.

- The Pact in its implementation should be connected to discussions in other Summit tracks, and other related fora and processes, including but not limited to the Code of Conduct on Information Integrity, the World Summit of the Information Society+20 Review, and on AI governance. It should proactively integrate other communities working on relevant issues to mitigate the difficulties faced by civil society and small, island, and developing states, which lack the resources to track multiple, simultaneous processes.

- The Pact should advance efforts within the UN itself to adopt and implement human rights due diligence requirements and protocols for all procurement, development, and use of new and emerging technologies.