SUBMISSION OF INPUTS FOR THE GLOBAL DIGITAL COMPACT

by the Global Digital Justice Forum

April 2023

CONTENTS

ABOUT

The Global Digital Justice Forum is a multisectoral group of development organizations, digital rights networks, trade unions, feminist groups, corporate watchdogs, and communication rights campaigners [including, Campaign of Campaigns, Development Alternatives with Women for a New Era (DAWN), Equidad, ETC Group, Global Policy Forum, Groupe de Recherche Pour Une Stratégie Économique Alternative (GRESEA), IT for Change, Just Net Coalition, Latin American Information Agency (ALAI), Oxfam International, Public Services International (PSI), Social Watch, The Centre for Research on Multinational Corporations (SOMO), Third World Network, Transnational Institute (TNI)] led by a digital justice vision.

This submission has been co-constructed by the group through the past several months of dialogue, deliberation and consultation with several communities in the Global South. It has also been circulated among partners and collaborators of the Forum's members, and validated by Asociación Latinoamericana de Educación y Comunicación Popular (ALER), Foro Argentino de Radios Comunitarias (FARCO), Global Initiative for Economic, Social and Cultural Rights (GI-ESCR), Internet Bolivia, Internet Ciudadana, and Pressenza.

The group has been working together to build a Global South perspective on digital technologies through policy engagement spanning local to global levels, including UN forums – on Internet and data, biodiversity and environment, trade, labor rights, gender equality, development cooperation, SDGs, global governance, multilateral reform, etc.

The work of the group (individually and collectively) over the past two decades – predating the World Summit on the Information Society (WSIS) process – is informed by a vision towards and practical action for:

a) democratizing the governance of digital technologies and promoting decentralized digital systems;

b) upholding the Internet as a global commons that can decentralize knowledge and power in our society and economy, enabling global exchange of information and knowledge, vibrant peer production cultures, sustainable local economies, free expression and association, and democratic deliberation and participation;

c) privileging a people-led, ecologically responsible, non-extractive, rights-enabling and gender-just vision of technology models that furthers a new international order rooted in development sovereignty;

d) calling for an end to corporate impunity; and

e) developing legal-policy frameworks for data, AI, and platforms grounded in human rights and economic justice on both transversal technological aspects and domain-specific/sectoral issues.

The members of the Global Digital Justice Forum consider the GDC as an important milestone that could (as the UN SG asserts in his Report to the Commission on Science, Technology and Development) become "an opportunity for Governments and other stakeholders to revitalize international cooperation in the light of the dramatic changes that have taken place in digital technology since WSIS" (Para 98, A 78/62-E/2023/49).

We believe that for this opportunity to materialize, the GDC must unequivocally reject the 'equal footing' multistakeholder model that has dominated digital cooperation processes, leading to an entrenchment of corporate power. Instead, it must build on WSIS outcomes, which still remain valid. The GDC must set up a new democratic global digital governance framework founded in a human rights-based constitutionalism that acknowledges the legitimate role of governments in digital policymaking.

The Global Digital Justice Forum sees a strong and central role for civil society and the social movements in global to local digital policymaking. As acknowledged by the WSIS, the Internet is a unique artifact, and a communication commons belonging to the people of the world. We believe that there is no digital cooperation without the participation of people in agenda-setting for an equitable, inclusive, and development-oriented digital society. The standpoints of those at the margins of society must inform processes towards the GDC. The multilateral system and governments need to use the creative potential of the Internet to ensure that such participation is not just notional, but as democratized and meaningful as possible, so that policies are agile, accountable, and attentive to people and the planet. The so-called digital divide is fundamentally a development divide. The commitments of the international community in delivering the 2030 Agenda should not be derailed or undermined by or be dependent on digitalization. Rather, the GDC must strive to ensure that digitalization is a positive force for the right of all to live well with dignity.

The members of the Global Digital Justice Forum, on the basis of their committed engagement on digital justice, seek to contribute to the GDC process to co-evolve the norms, principles, and policies for a future digitality based on a commitment to the integrated and indivisible human rights agenda, including, the right to development, pluralism of knowledges, wellbeing of planet and people, and human flourishing.

Some instances of the work we have done:

- Delhi Declaration
- Digital Justice Manifesto
- Declaration of Feminist Digital Justice
- Food, Data and Justice Dialogues
- Digital Colonialism - analysis of EU trade agenda
- Gender-transformative Digital New Deal
- Economic Rights in a Data-based Society
- A 20-point agenda towards a just and sovereign digital future

Submission of Inputs for the Global Digital Compact by the Global Digital Justice Forum

Thematic Areas

1. Connect All People to the Internet, Including All Schools

Problem Statement

The current connectivity paradigm led by Big Tech is based on an extractive neoliberal market logic. Its centralized server-client model, predicated on behavioral engineering to valorize user attention for private profit, has thwarted the empowering potential of the Internet for social transformation. The Big Tech model also comes with unsustainable environmental costs – from strip mining of rare earth minerals in conflict zones for development of hardware to huge resource requirements and GHG emissions footprint generated by the global data centers of Internet corporations.

Principles

1. Universal, equal, non-discriminatory, quality access to the Internet and data is a human right.
2. Connectivity must lead to a fair, inclusive and equitable digital society and economy that promotes agentic participation.
3. Children must not be exposed to unaudited algorithms, as their vulnerability to harm is greater. Such algorithms also dilute teacher agency and must be banned in school education.
4. Respect for planetary boundaries and ecological well-being must be a central principle in digital innovation systems and infrastructure development.
5. The governance of digital, data, and AI infrastructures must privilege public accountability, community control and voices of the marginalized, underscoring both individual and collective rights in relation to the ownership and management of digital resources.

Goals

1. To ensure that connectivity results in substantive inclusion and democratization of the Internet's value propositions through public financing models.
2. To promote the development of empowering user cultures, critical digital literacy, and meaningful digital enskillment, including in schools at all levels.
3. To enable alternative platformization pathways for a just digital transition.

Actions – Multilateral System

1. Introduce a Digital Development Tax for a democratically governed Digital Solidarity Fund: this would entail compulsory contributions from dominant digital services firms to finance public digital infrastructure in developing countries. This can be a pool created from taxes on market share of digital transnational corporations (TNCs) (across different Internet services layers) and fees levied on Internet registries for domain name sales etc.

2. Redefine the mandate of international financial institutions to meet the challenges of a new epoch, providing assistance to build autonomous platform and data infrastructure which supports digital industrialization in the global South. Eradicate tax havens to realize adequate revenues for fairer digital societies.

Actions – Governments

1. Set up and effectively utilize a Universal Service Obligation Fund (USOF) with gender budgeting to ensure universal access to the Internet as a public service, including through public access and data allowance programs.

2. Regulate Internet Service Providers to ensure non-discriminatory and affordable access. This includes through rules for zero services business models, price caps on broadband services, obligatory private infrastructural investment, and a tax on transnational Internet services providers and investors of foreign direct investment (FDI) in digital sectors. These measures can support zero-cost access programs in remote, rural and underserved geographies.

3. Invest in the creation of digital public goods, and models for connectivity and services involving participatory approaches and public-community partnerships.

4. Create a positive regulatory and policy environment for community-owned networks of all kinds, including the use of USOF funds.

5. Develop policies and standards, including due diligence guidance for digital services corporations, to eliminate algorithmic and ecological harms in digital value chains, and encourage environmentally-friendly digital services and innovation.

6. Build critical thinking capacities, digital literacy and media literacy among children and youth, including through the public education system, also investing in public digital resources to create a rich learning environment which is not controlled by for-profit corporations.

2. Avoid Internet Fragmentation

Problem Statement

Big Tech-led standards processes for the embedded Internet, like the Metaverse Standards Forum, further the consolidation of the privatized walled gardens of platform behemoths. The WSIS agenda of internationalizing the technical governance of Critical Internet Resources remains incomplete, due to the flawed Internet Assigned Numbers Authority (IANA) transition process in 2016, with ICANN remaining under US jurisdiction. Also, given the lack of progress towards a multilateral mechanism for Internet-related public policy issues, the 'enhanced cooperation' agenda from the WSIS remains unfinished. Against this backdrop, unilateral actions of governments (for instance, the US-China standoff) heighten the risk of a 'Splinternet'.

Principles

1. The Internet must be preserved as an open, secure, free and equitable global commons that can neither be enclosed by private platforms nor misused to undercut human rights and global peace for narrow political ends.

2. In accordance with the WSIS consensus:

    a. A democratic governance framework must be designed for global Internet governance, rejecting outright the failed model of 'equal-footing multistakeholderism' that has given Big Tech an illegitimate seat at the policy table.

    b. Sovereignty of state parties on Internet-related public policy issues must be respected in Internet governance processes at the international level.

Goals

1. To put the WSIS consensus into action (Para 48 of the Geneva Declaration of Principles & Para 70 of the Tunis Agenda) for - a) effective internationalization of technical policy issues in Internet governance (pertaining to Critical Internet Resources, including, in particular, Internet names and addresses), and b) a separate mechanism for 'enhanced cooperation' distinct from the Internet Governance Forum (Para 69 of the Tunis Agenda).

2. To develop binding technology standards based on democratic deliberation at the multilateral level to prevent Internet fragmentation.

Actions – Multilateral System

1. Accord jurisdictional immunity to ICANN and rescind the clause in the IANA transition agreement that requires its incorporation in the US. Re-incorporate ICANN as an international entity akin to the Red Cross.

2. Revise and expand the International Telecommunication Regulations (ITRs) to include binding international standards on network-data technologies (such as interoperability, security, personal data protection, quality benchmarking etc.) for adoption by all countries, effectively replacing voluntary guidance mechanisms such as the ITU Telecommunication Standardization Sector (ITU-T) focus group on metaverse.

3. Set in motion a plan of action to reaffirm and implement the July 2022 resolution of the Economic and Social Council that commits to pursuing enhanced cooperation, as distinct from the Internet Governance Forum (IGF), including preparatory guidelines for WSIS+20.

3. Protect Data

Problem Statement

The clickbait model to valorize user attention for private profit has permeated the entirety of the digital services economy today. Consent frameworks place an unreasonable burden on individuals to be vigilant about their data. Corporations exploit this to their benefit, including through dark patterns in the design of digital services, nudging users into the net of behavioral surveillance. These trends suggest a deep vitiation of the democratic social fabric.

Traditional approaches to data protection that limit privacy harms to non-consensual data processing and re-identification of the data subject are not adequate to safeguard individuals and society from data harms. Evidence suggests that even without re-identification, there are a host of individual/collective harms that emerge from group profiling (such as denial of rightful entitlements in algorithmic sorting of welfare recipients or social credit scoring in digital financial services targeted at vulnerable populations).

Principles

1. Privacy and personal data protection frameworks must effectively address the erosion of individual, collective and societal autonomy arising from a) non-consensual data collection, b) individual and group profiling, c) recombination, third party sharing, and downstream processing of anonymized personal data.

2. The digital economy must be effectively regulated to prevent enclosure of the social commons of data resources and allowing powerful actor to capture the benefits accruing from it.

3. The protection of data must include the sovereign right of peoples and communities to own, control, generate value, and benefit from their data resources.

Goals

1. To evolve appropriate international and national frameworks to protect people's right to privacy and data sovereignty.

2. To ensure that the creation of digital public goods/infrastructures at the global and national levels is backed by robust safeguards to protect privacy and personal data, enhance autonomy, and promote equitable benefit sharing.

3. To ensure that laws and policies for data governance maximize social benefit and curtail market tendencies for concentration and exploitation.

Actions – Multilateral System

1. Institute a binding global governance framework in relation to digital human rights, which includes –

    a. No-go areas where the data market cannot operate.

    b. The right to encryption and freedom from commercial surveillance as integral components of the right to privacy.

    c. The right of communities to steward their data resources as an integral part of their Economic, Social and Cultural Rights (ESCR).

    d. Recognition of state requirements for mandatory general client-side scanning of communication as a disproportionate and intrusive violation of privacy (A/HRC/51/17 2022).

2. Update the International Labor Organization's (ILO's) Code of Practice on Workers' Personal Data (1996) in dialogue with unions to ensure that privacy safeguards are adequate to worker autonomy in algorithmically mediated workplaces. This must address worker data rights, including the rights of unions to access all algorithms, freedom from disproportionate data surveillance, the right to explanation and appeal to challenge automated decision-making, the right of unions to engage in algorithmic audits, and obligations of employers to negotiate with unions on the introduction of surveillance tools.

3. Mandate ex-ante human rights assessments and gender audits – with particular attention to 'do no harm by design' and 'data privacy and security principles' – in the Digital Public Good registry of the UN Digital Public Goods Alliance (DPGA).

Actions – Governments

1. Update national privacy frameworks to align with Convention 108 of the Council of Europe, to address the risks of individual and collective harms stemming from anonymized data processing, algorithmic sorting, and ranking systems adopted in a range of digital services.

2. Adopt the 'precautionary principle' in the development and deployment of all data public goods and AI innovations.

3. Institute robust safeguards of necessity, proportionality, and legitimacy in welfare targeting, and prevent intrusive profiling of vulnerable populations.

4. Apply Human Rights Online

Problem Statement

Cyberspace mirrors and amplifies social exclusion and discrimination based on class, race, gender, caste, and other axes. The rights of women and less powerful/ oppressed groups are under threat in the digital public sphere due to algorithmic virality and the intensification of hate. Multistakeholder frameworks such as the Christchurch Call have proven ineffectual in addressing this.

Social power which characterizes our hybrid existence in the digital epoch cannot be explained through an approach that considers the online analogous to the offline. While the values that underpin the human rights approach to a humane and just society are abiding, it would be simplistic to equate the rights scaffolding pre-digital life with those in the fluid social context constitutive of digital life. Further, the rights of individuals and communities who have no online presence are also violated because of data harms arising from digital intelligence held and used by state and private actors.

The datafication of our bodies and social interactions requires an imagination of our individual and collective sovereignty to protect both privacy rights in relation to data and democratic governance of data as the new social knowledge. The global governance gap in cross-border data flows has reinforced global inequalities, as data resources from countries of the South are cornered by a handful of Northern corporations. The human rights framework hence requires an update that is adequate to digitality through a new class of rights in relation to data and data sovereignty.

Principles

1. The digitally-mediated public sphere must be free from all forms of hate speech, racialization, form of social discrimination, and violence, including sexism.

2. The international human rights framework must be updated to incorporate, as appropriate, a new class of data rights to protect political, social and economic freedoms in the space of flows.

3. In an interdependent world, the principle of solidarity requires that all countries and peoples have a right to benefit from the gains of digitalization. The consolidation of data power in the hands of a few countries and their corporations must be addressed through new policy and legal frameworks for data equity and justice.

Goals

1. To update the human rights framework to accommodate a new class of data rights and ensure accountability from state and non-state actors for enforcing these rights.

2. To bring the multilateral system up to speed on human rights and data governance.

Actions - Multilateral System

1. Adopt a binding consensus to enforce corporate accountability for preventing hate speech and incitement to discrimination, hostility and violence in platform environments, including algorithmic content moderation and curation.

2. Issue guidance on what constitutes sexist hate speech and technology-facilitated gender-based violence through a Convention on the Elimination of All Forms of Discrimination against Women (CEDAW) Committee General Recommendation.

3. Build a data rights constitutionalism that defines new typologies of rights at the intersection of digitalization/ datafication and traditional human rights discourse. This, inter alia, will include the right to data access, the right to explanation, the right to be forgotten, the right to be represented (or not) in digital systems, the right to participate in decisions about data innovations, protection against all forms of data discrimination including unfair denial of citizen entitlements, and workers' data rights in algorithmic workplaces.

4. Explicitly acknowledge the sovereign right of peoples to govern their data resources towards the progressive realization of ESCR, and as an extension of state parties' right and duty towards development of its people.

    a. The UN Convention on the Right to Development being negotiated under the auspices of the Human Rights Council (HRC) must recognize the breach of people's data sovereignty as a violation of their right to development.

    b. The policy frameworks related to trade, intellectual property, taxation, and international development in areas such as health and food systems must be fit to address the inequity of data and AI infrastructural power, and enable the furtherance of open and flourishing digital futures.

5. Mobilize public financing and introduce a new taxation regime to enable developing countries to participate equally in the international digital order.

Actions - Governments

1. Adopt a national data constitutionalism rooted in human rights to guide all sectors of the economy and society.

2. Introduce content governance frameworks, including human rights-based benchmarking of harmful content that takes into account contextual and intersectional manifestations of hate speech, and establishes corporate accountability to protect digital human rights.

3. Invest in digital policy development and public infrastructures to maximize and democratize data capabilities and innovation.

5. Accountability for Discrimination and Misleading Content

Problem Statement

The private and closed content streams of mainstream platform models have destroyed the generative web of hyper-links that is founded on a pluralistic openness. The dominant business model of platforms built on surveillance advertising deploys algorithmic personalization, amplifying and intensifying social bias and intersectional discrimination.

Section 230 of the US' Communications Decency Act, which treats social media/ digital services platforms as neutral conduits, has become a precedent in most jurisdictions. It enables powerful corporations to evade their accountability for the proliferation of algorithmic hate and misinformation and escape public scrutiny.

The appropriation of the Internet by state and non-state actors for propaganda has resulted in the weaponization of content, feeding authoritarian populism and destroying the social fabric.

Principles

1. The web we want is an open, diverse, equal Internet that promotes the freedom of expression and information, media pluralism, and a diversity of knowledges.

2. The independence of public and private media services must be guaranteed to prevent the unjustified removal of media content by state agencies or large online platforms.

3. The defense of platform neutrality must be limited only to Internet intermediaries who do not engage in content governance and are neutral to the content they carry (for example, Internet service providers, hosting services etc.). Social media and digital services platforms that actively engage in content moderation and curation must be held accountable for the content governance actions they perform, including through the deployment of the algorithms they own. News media aggregators and online publishers must be governed by publisher liability rules to prevent the circulation of harmful content without encroaching on media freedoms.

4. Automated content curation and content moderation systems must be based on human rights frameworks, and subject to transparency and accountability. Users must have the right to a) contest the decisions made by such systems, b) receive explanations for how tensions or conflicts between different values were balanced (freedom of expression vs privacy and so on) and c) seek redressal in case of unfair decisions.

Goals

1. To shift out of a 'walled gardens' paradigm to new platform models that are open, secure, interoperable, and autonomy-enabling.

2. To overhaul Internet intermediary liability frameworks at global and national levels so that safe harbor protection for digital services platforms is contingent on the fulfillment of human rights obligations in their algorithmic content moderation and curation systems.

Actions - Multilateral System

1. Evolve a binding human rights-based content governance paradigm for the transnational communications agora of the Internet that holds states and corporations to account for human rights violations.

2. Strengthen the proposed UNESCO Guidelines for Regulating Digital Platforms (intended to serve as a model code for content governance) by including the following aspects:

    a. Mandatory human rights compliance and periodic due diligence for platforms.

    b. Interoperability obligations and a duty of transparency in respect of both algorithmic content moderation and content curation functions performed by digital platforms, and duty to cooperate with public audits by independent national regulators.

Actions - Governments

1. Based on a human rights-based intermediary liability framework, set up an independent national agency for the effective regulation of automated content moderation and curation systems of digital services platforms (whether owned by state or non-state actors) with the mandate to:

    a. Prevent de facto opt-ins into algorithmic personalization, and guarantee data portability.

    b. Review content take down orders by state agencies for impact on user freedoms.

    c. Ensure that rules for algorithmic recommendation systems of digital services platforms encode crucial public interest values such as media pluralism and diversity, and not just focus on maximizing user preference and choice.

    d. Develop and implement an independent public AI system for automated content moderation based on public standards and weightages, which are open to scrutiny and built through public deliberations. This should be the 'reg-tech' for all public and private digital media services operating in a particular context.

2. Introduce legislation to provide safeguards to digital media publishers against political interference in editorial decisions and surveillance. (The proposed EU Media Freedoms Act is a notable development in this regard).

6. Regulation of Artificial Intelligence

Problem Statement

AI risk-mapping is guided by an unhelpful long-termism. This, in effect, has seen the proliferation of a discourse of 'ethical AI', which, even if useful, is unable to address the here-and-now damage caused by the concentration of economic and political power, and entrenchment of social inequities in the design and deployment of AI systems. The dual-use nature and possible misuse of AI technologies in the military domain by states and non-state actors also presents a real threat that the multilateral system has not tackled front and center.

There is a growing gap in technological capabilities between countries that are AI leaders and those lagging behind in technological advancement, which is exacerbated by current IP regimes that impede AI development for public and social ends.

Principles

1. No AI is too powerful to evade public oversight.

2. The 'precautionary principle' used in environmental law and used by the EU in its AI regulation must guide the

research and deployment of AI systems in all sectors.

3. Instances of AI use that pose grave threats to peace, security, human and ecological well-being must not be permitted at any cost.

4. The social value of AI must accrue to the communities from whose data footprints that digital intelligence has been generated.

Goals

1. To institute mandatory ex-ante and ex-post assessments of risks to human rights and threats to peace and security in relation to specific uses of AI at every stage in their development.

2. To decentralize AI innovation by breaking AI monopolies, and institute public financing mechanisms to build the technological capabilities of developing countries for democratizing AI's economic and social value.

Actions - Multilateral System

1. In line with the precautionary principle, accelerate the formalization of binding regulations on Lethal Autonomous Weapons Systems and institute a global ban on non-human control of nuclear weapons platform launches.

2. Evolve binding common standards and approaches through the development of a common global architecture to guide future trajectories of AI design, development, and use.

3. Reject digital trade rules that prevent nation-states from enforcing transparency and accountability regulation on AI services and application providers (such as the prohibition on source code transfer).

4. Reform Intellectual Property Regimes and introduce new licensing systems similar to the creative commons regime so that community contributions are recognized in the development of generative AI. For instance, the Maori Whare Kōrero Kaitiakitanga License prescribes that derivative products created from linguistic datasets co-generated through community contributions must be available for community use and returned to the common pool.

5. Bridge the AI divide between nations through international public financing initiatives that encourage contextually appropriate and accountable AI models.

Actions - Governments

1. Mandate compliance with algorithmic accountability and transparency regulation as a precondition for transnational AI service providers to have market access, especially in developing countries.

2. Safeguard transparency and accountability of AI systems through AI accountability legislation. Sector-specific guidance for operationalizing rules for various AI applications and services must be issued.

3. Promote a capabilities approach to digitalization that recognizes investments in techno-institutional infrastructure and human capabilities as the twin strategies for the AI paradigm.

7. Digital Commons as a Global Public Good

Problem Statement

The multistakeholder model of global Internet governance is riven with multiple conflicts of interest, as private sector actors whose profit imperatives clash with the wider public interest are given an equal seat at the policy table. The attempt to create an IGF leadership panel to communicate policy decisions from the IGF to appropriate policy forums goes against the WSIS consensus, and has the perverse effect of leading to a situation of Big Tech governing itself. This will perpetuate the status quo of corporate enclosure of the Internet commons.

Global data public goods being created in the UN system (in the health and food systems, for example) lack robust institutional frameworks that can prevent free-riding and enclosure of their value by powerful corporations.

Unrestricted cross-border data flows impede developing countries from furthering their infrastructural capabilities to leverage their data commons for autonomously defining pathways to development.

Principles

1. The global knowledge commons of the Internet must be governed democratically in order to ensure that the social value generated can enshrine democracy, equality, and the right to participation and community for all peoples, especially those at the margins of society.

2. Global data public goods being created in the UN system must be backed by robust institutional frameworks to prevent free-riding and enclosure of their value by powerful corporations.

3. Data sovereignty is development sovereignty. All nation-states must have the policy autonomy to evolve domestic data governance regimes for their infrastructural development.

Goals

1. To actualize the right and duty of all nation-states to uphold a democratic global digital governance regime through a multilateral, people-centered, public policy mechanism for Internet, platform, data and AI technologies, free from corporate capture.

2. To develop a new approach to the governance of data which recognizes networked data resources as a knowledge commons. Networked data refers to the aggregate social knowledge continually co-generated by individuals through their socio-environmental interactions.

Actions - Multilateral System

1. Catalyze an institutional process at the UN level to pursue the unfinished agenda of ‘enhanced cooperation’ in line with the WSIS Tunis agenda and to check illegitimate TNC interference in the sovereign policy space of state parties.

2. Set up a dedicated institutional mechanism at the multilateral level for access and benefit sharing, akin to the Nagoya Protocol of the Convention on Biological Diversity, for fair benefit sharing in global data public goods.

Actions - Governments

1. Provide key services such as email, video-conferencing, search engines, etc. as public goods, just like postal services and basic telecommunication services.

2. Evolve a resource governance regime for the economic governance of data and digital intelligence that is based on a common property resource tradition with appropriate guardrails to prevent enclosure.

3. Institute mandatory data sharing obligations on dominant platform companies that have enclosed huge amounts of data to tackle anti-competitive practices in the digital marketplace. Reform competition law for structural separation of data value chains, in addition to horizontal separation of data service and marketplace layers.

4. Ensure that the maximization of data's public value does not lead to the intensified risk of individual and collective harms. National laws for the economic governance of data must be based on boundary setting so that human rights guarantees and community claims in the data commons are not traded away. There must be a clear separation of personal data protection regulators from institutional bodies that are entrusted with the task of managing common data pools and data exchanges.

5. Distribute the intelligence value derived from aggregate data resources to the relevant data communities from whose interactions or territories the data was originally extracted.

6. Prioritize the use of free, open, and interoperable digital infrastructures in public administration.

7. Promote alternative platform models, including cooperatives and social enterprises, to enable decentralization of data value for vibrant local economies.

8. A Feminist Approach to the Digital Transition

Problem Statement

An instrumentalist view of digital technologies has resulted in an ecologically destructive and socially untenable world that is rife with gendered exploitation, normalization of precarity, and a breakdown of the social contract.

Principles

1. Make a Southern feminist vision of gender justice a central principle of the Global Digital Compact – see here.

Goals

2. To design a new socio-institutional architecture of digitality that respects the human rights, dignity, and agency of all people as well as the rights of nature inherently associated with natural ecosystems and species.

3. To address the lack of a social care infrastructure in the economy of ubiquitous hustling.

Actions - Multilateral System

1. Invest in alternative platform, data, and AI models rooted in values of local accountability, indigenous modes of knowledge production, women's participation and ecological sustainability. This can be achieved through the STI for SDGs strategy roadmaps and work programs.

2. Harness the Internet and the social resource of data and data-based intelligence as a future-ready force for gender-transformative, ecologically compatible development if Agenda 2030 is to be realized.

3. Reform the international taxation regime to stop base erosion and profit shifting practices of transnational digital corporations, in order to enable states in the global South to generate adequate fiscal revenues for social care infrastructure.

Actions - Governments

1. Adopt and enforce feminist economic policy measures that apply not only to the world of work, but also recognize the human right to care, redistribute care work from families to public services, and obligate the state to provision care systems and services as a public good. The ILO's 5R Framework for decent care work is an important starting point. Without this, exploitation of women's labor and unpaid care work in the platform economy cannot be stopped.

2. Prioritize investments in platform and AI models that address social bias and promote gender equality.