IGF MESSAGES

Addis Ababa, November/December 2022

The following document is a preliminary summary of points raised during the Internet Governance Forum in Addis Ababa, 28 November to 2 December 2022

It is a work in progress, provided for information only on the final day of the IGF

A draft document of IGF Messages from the Forum will be circulated for consultation by 16 December 2022

The views and opinions expressed herein do not necessarily reflect those of the United Nations Secretariat. The designations and terminology employed may not conform to United Nations practice and do not imply the expression of any opinion whatsoever on the part of the Organization.
Connecting All People and Safeguarding Human Rights

Digital Divide

- The digital divide is much more than a connectivity divide. Meaningful access includes issues of accessibility, affordability, content, services, digital literacy and other capabilities as well as connectivity.

- The COVID-19 pandemic demonstrated the Internet’s role in enabling individual and economic resilience, but also illustrated that those who lacked connectivity or meaningful access were disadvantaged.

- Only 21% of people in Least Developed Countries (LDCs) are estimated to make use of some access to the Internet in 2022, compared with 81% rate in developed countries.

- Some groups within society experience more extensive digital divides. Women in many societies are less connected than men. Digital disadvantage is exacerbated among vulnerable groups such as older people, those with disabilities and refugees. Targeted initiatives can help to improve the access rates for such social groups.

- Access needs to be affordable, reliable, and appropriate. Affordability is an issue in much of the Global South. In Africa, large distances between rural communities makes connectivity more costly, as last mile connectivity is often unattractive to the private sector. Community networks and other innovative approaches can address this.

The Gender Digital Divide

- Men are significantly more likely to be online or have mobile connectivity than women, and the gap being considerably higher in the Global South and in LDCs. The Sustainable Development Goal target for universal Internet access cannot be met until this gap is closed.

- The mandate of IGF Women is on the right track - notions of gender equality, inclusion, and women’s rights and protection must be incorporated into the Global Digital Compact.

- Before laws and policies are considered, the priority should be to identify the morals, principles, and values that guide the Internet’s use.

- The threat of violence and harassment is a deterrent to women’s online participation. The role of technology services and platforms in propagating gender-based violence must be acknowledged and addressed.

Human Rights

- Universal access must be achieved without leaving digital rights aside - one way of doing it is by embedding the latter in internet governance structures. This is crucial to ensure the Internet is both an accessible and safe space for all.

- Efforts to improve connectivity, particularly in the Global South, must be aligned with human rights: including freedom of expression and association, the right to privacy and other civil and political and economic, social and cultural rights.
Resilient Infrastructure

- Resilient digital infrastructure is crucial for digital inclusion. It will take time and investment resources to improve its capacity. Regional infrastructure imbalances need to be addressed, particularly those for rural areas, including power as well as communications infrastructure.

- Governments should focus on protecting infrastructure and developing capacity through multistakeholder collaboration. This requires efforts to address constraints posed by telecommunications monopolies and market concentration to establish regulatory agencies and frameworks and to encourage community networks to provide connectivity through businesses and NGOs.

Education and Labour

- The quality of education in the Global South, particularly during the pandemic, has suffered due to a lack of connectivity. While ICTs can ensure meaningful access for students, differences in global adoption rates have exacerbated pre-pandemic inequalities.

- Use of digital tools by small and medium-sized enterprises has increased greatly since 2020, but micro-enterprises still face significant challenges in their capacity to digitalise their businesses.

- The gig economy presents many opportunities for job creation for women - who occupy the informal sector more than men - but lack of training remains a barrier.

- Improving ICT infrastructure and access is not enough for better education and job creation. Digital competencies must be improved, and adaptations in teaching and learning methodologies are needed to adapt to the new digital paradigm of education.
Avoiding Internet Fragmentation

- There is widespread agreement within the Internet community on the value of a global, unfragmented Internet as a platform for human activity. The GDC is an opportunity to reassert the value of an open interconnected internet for the exercise of human rights, realisation of the UN Charter, achievement of the Sustainable Development Goals and exercise of human rights.

- Fragmentation is a layered discussion, with different stakeholders applying a variety of meanings and interpretations to the term. Respect and understanding for different people’s understanding and experience of fragmentation is essential in reaching coordinated, effective responses.

- A wide range of political, economic, and technical factors can potentially drive fragmentation. However, diversity and decentralisation should not be mistaken for fragmentation - these are fundamentally positive aspects of the Internet’s architecture and operations.

- Effective multistakeholder governance mechanisms are essential for the governance of a global unfragmented Internet. There is a need to re-enforce trust in those mechanisms, and ensure that they are robust and sustainable, and to foster coherence across governance structures as they evolve to meet new challenges.

- While legal, regulatory and policy approaches will differ around the world, active coordination is vital for ensuring that fragmented approaches do not threaten the global reach and interoperability of the Internet.

- There is a strong need for vigilance with regard to new or developing fragmentation risks. Global cooperation and coordination will be essential in identifying early warning signs, mapping the impact of certain policies or approaches, and being ready to take preventive action. The IGF Policy Network on Internet Fragmentation is a positive example of this work.

- A multistakeholder approach is best suited to assess, evaluate and monitor for unintended consequences of measures pursuing legitimate purpose and suggest effective alternatives that do avoid the risk of fragmentation.

- Many factors affect the experience of the Internet in different jurisdictions. The pursuit of digital sovereignty, in some forms, can increase the risk of fragmentation at the technical level of the Internet.
Governing Data and Protecting Privacy

The centrality of data: the digital commons, global digital public goods, digital economy and SDGs

Data is a critical resource in the hybrid digital age. Analogies of data as the new oil, gold or currency signify its centrality in driving economic growth and influencing social values. Big data analytics, AI systems, and innovations across SDGs and public policy dimensions demonstrate the need for appropriate political considerations and nuanced policy interventions.

Data flows are critical for international cooperation in many fields, such as scientific research, law enforcement, national and global security. The effective use and sharing of data on a global scale can help overcome shared challenges and cascading crises such as climate change and pandemics.

Data poverty remains, especially in local communities and among vulnerable segments of populations. Data management and governance are complex issues in both national and transnational governance.

Protecting data privacy to upholding data justice

Data privacy is not a matter of convenience or good practice but of human rights - including the rights to privacy, equal treatment and non-discrimination as well as access to other fundamental rights such as healthcare, and democratic rights such as free expression and association. Privacy and data protection are central to the governance of AI, and all stakeholders in the AI supply chain have a role to play in upholding privacy rights. We should reach beyond data protection to data justice people have choices over how personal data are used and where they can also share the returns and benefits of innovation brought by those datasets.

The privacy of personal data is often sacrificed in data exchange, between collection and application, with intentional or unintentional consequences for trust and security. Data flows and exchange should take place without compromising data privacy. These requirements are not contradictory, and both objectives should be supported simultaneously. Privacy protections should contribute to a safer and more prosperous digital economy.

Authorities need to ensure that personal data is protected, and measures are implemented in a way that does not impose burdens on individual responsibility, with clear, differentiated responsibility of different stakeholders.

There is a need for independent oversight bodies (such as data protection offices) equipped with appropriate resources. Data protection offices could be institutionalized with a mandate to resolve complaints from data subjects, providing guidance, implementing investigations, and managing data registration.

Privacy laws should be concrete, evidence-based and not abstract. Those affected by them should understand them clearly. Datas governance policies should be developed with multistakeholder input to understand these implementation challenges.

From silos to holistic, multistakeholder approach in governing data

Issues concerning data governance should not be treated in silos or isolation. For instance, data rights go hand-in-hand with rights to equal treatment and non-discrimination, as well as access to health, education
and basic services. Data rights go hand in hand with human rights --- when data rights are not respected, human rights are at risk.

**Important considerations in governing data include (but are not limited to):** data standards and classification; data sharing, exchange and interoperability; data security and data privacy; data infrastructure; data and digital identity; data justice and fairness; data traceability, transparency and explainability; data minimization versus data limitation; data life cycle, data use specificity and retention; data accuracy and quality; data bias, marginalization and discrimination; data accountability versus data ethics; data harms, data security and data protection, etc.

**Existing legislation and frameworks at national, regional, and international levels are insufficient. Current legislation processes are lagging,** failing to keep up with the fast pace of various digital transformations.

**The current data governance landscape is also highly fragmented** (ranging from state control to private sector control to individual control), a patchwork of national, regional, and international rules. Greater coherence is needed on a global level.

Different contexts and challenges, different histories, cultures, legal traditions, and regulatory structures mean that there cannot be **one rigid set of rules for all.** Furthermore, different individuals and organisations will interpret the same approaches in their own manner. However, as countries and regions develop their own tailored approaches to data governance there should be some level of consistency and interoperability to facilitate data flows and ensure that the playing field is equal.

**Actors and stakeholders including regulators, researchers, standards organizations, and end users have respective roles to play and should exercise their power and influence to promote effective data governance.** Policies for data governance should be developed with input from the multistakeholder community which has expertise not only the abstract legal debates around privacy but also the “real world” challenges of implementing effective data privacy solutions.

**There is a need for safe and honest spaces of conversation at the intersection of digital technologies and security policies, such as the UN IGF and NRIs.** The responsibility to create this space falls on the entire multi-stakeholder ecosystem: Civil society, academia, private sector, governments and technical community, as well as international and intergovernmental organizations.

**Enabling equitable cross border flows**

**Efficient intra-regional trade and supply chain management rely on the smooth flow of goods, services, capital, as well as data.** Cross-border data flows are essential to many aspects of e-commerce and digital trade. However, these require complex cross-cutting considerations for regulatory convergence, harmonization of legal frameworks, Internet governance, information and communications technology (ICT) policy reform and strategic regional ICT infrastructure implementation.

**Current multilateral, bilateral or regional trade agreements are insufficient to address cross-border data flows.** These operate in a largely unregulated environment with little consistency between national legal regimes. Approaches differ and are contextual, generating barriers to trade. There is an increasingly critical need to harmonize and develop outcome-oriented international measures, respecting national sovereignty and addressing context-specific needs. Many countries also do not have sufficient enforcement capacity.

There is a need for interoperability between different data privacy regimes. While one size may not fit all, some level of consistency and interoperability is necessary to ensure that data moving across borders are effectively protected.
Integrated national data governance frameworks

Developing economies need to enhance the institutional capacities to govern, use and manage data in a comprehensive, objective and evidence-based manner, including through regional and global cooperation. There is an equally important need to build awareness about the institutional capacities of government officials and stakeholders in countries.

Trust, data literacy and data capacities

It is necessary to build data literacy and data capacities across levels of governments and for the general public. Institutions should be equipped with infrastructure to implement effective, integrated national data governance frameworks. Trust is at the center of data governance and is lacking due to lack of data literacy. There is often public trust deficit due to the inadequacy of data protection.

Data are integral to every aspect of the modern world, including for youth and children. One third of Internet users are below 18, and application developers have the burden of ethical and safe design - especially regarding targeted advertising to children. Building data literacy should be included in different levels of education including primary, secondary and tertiary levels.

Recent trends and development

- The Digital Single Market as envisioned by the AU Digital Transformation Strategy 2020-2030, is a bold and long-term vision that requires the commitment of not only Government but all stakeholders to bring it to fruition. In collaboration with UN ECA, an integrated data policy and an interoperability framework for digital ID has also been developed.
- The Digital Trade Protocol negotiations will be considered in December 2022 as part of the African Continental Free Trade Area (AfCFTA).
- It is also recommended to accept the principles like the Data Free Flow with Trust (DFFT), in both national and international data strategies. It is suggested to promote data governance as a regional agenda in regional institutions and among neighboring countries.
- The African Regional Center on Artificial Intelligence has been launched in the Republic of Congo as a regulatory framework approach for data and artificial intelligence.
- The Cross Border Privacy Rules (CBPR) is one example of an effort to promote interoperability. (see globalcbpr.org)
- Reference is made to current UN’s capacity development efforts in helping low and middle-income countries to plan and implement integrated national data governance frameworks, with coherence to regional and global frameworks.
Enabling Safety, Security and Accountability

Cybersecurity-cybercrime (role of policy makers)

- Prevention of cybercrime, and improving cybersecurity, are both important initiatives that merit serious attention and require the development of expertise. However, the approaches to each of them will differ: an approach that is functional in one area, will not be functional in the other without adaptation and rethinking.

- States should take care to avoid developing cybercrime laws that may negatively affect the work of cybersecurity defenders. They should invite other stakeholders to their conversations and enable an ongoing learning activity between the different communities involved.

- Civil society should participate in both cybercrime and cybersecurity discussions. To do so effectively, they should and educate themselves on the different approaches and issues involved and work with other stakeholders gather the information and resources required.

- Cybersecurity and cybercrime issues have cross-organisational and cross-border dimensions. Tackling these requires:
  a. Whole-of-government and whole-of-society approaches involving strong partnerships and coordinated efforts including parliaments, relevant authorities and agencies, the private sector, the technical community, academia, and civil society.
  b. Efficient and effective regional and international cooperation, both intergovernmental, multilateral and multistakeholder.

Cybersecurity

- Tensions between the desire to advance digital transformation and the need to enable effective cybersecurity pose risks to achieving a safe, secure online environment and the Sustainable Development Goals. While doing more to increase the resilience of digital infrastructure is necessary, it is not sufficient. The international community should explore practical ways to mainstream cybersecurity capacity building into broader digital development efforts. Translating existing international agreements into feasible actions is long overdue.

- Modern Internet standards are essential for an open, secure and resilient Internet that enables social progress and economic growth. These standards are readily available, but their use needs to grow significantly to make them fully effective. The United Nations is urged to help accelerate the global uptake of key standards, by including their promotion in the Global Digital Compact, and supporting advocacy and capacity building as well as initiatives to test and monitor deployment. This is particularly important to protect those who are not yet connected

- Listening to the experiences of victims and first responders of cybersecurity incidents is closely related and relevant to the Internet Governance Forum and ongoing UN-level Cybersecurity Norms deliberations. Cybersecurity norms must make a difference to the lived experiences of people, past, present and future.

- The Global Conference on Cyber Capacity Building (GC3B), scheduled for 2023, is an important opportunity to bring diverse stakeholders together to mobilise effective, sustainable and inclusive
stewardship of international cooperation for cyber resilience, including goals concerned with international development and international cyber capacity building.

- Stakeholders are encouraged to make use of the Global Forum on Cyber Expertise ecosystem and tools, such as the Clearing House, that not only match needs with resources, but also support stakeholders by clarifying their requirements.
- Opportunities to finance cyber resilience need to be addressed through different sources, while ensuring that resulting global public goods remain sustainable.

**Tackling cybercrime**

- Governments and policymakers should ensure that legal responses to terrorist use of the Internet safeguard both the rule of law and human rights, with consideration for freedom of expression, as well as encouraging transparency and accountability.
- Regulations countering cybercrime should be sensitive to the size, capacity and resources of platforms. Legal obligations should consider the diversity of the technical sector, and acknowledge the needs of smaller players in adhering to their legal obligations to counter terrorist and violent extremist exploitation of their services.

**Protection of women against online gender-based violence**

- Online gender-based violence is an important factor driving and reinforcing gender inequality in Internet access, leading to some women leaving online spaces. It is vital to equip women with guidance to resist online gender based violence, including through community led helplines. Resources, community guidelines and reporting on platforms need to be made available in local languages. It is also important to consider inclusivity, especially taking inter-sexuality and other vulnerable groups into account.

**Content / safety online / disinformation**

- Disinformation can and should be addressed while fully protecting freedom of expression, aware of the risk that measures suppress free speech and pluralism.
- Disinformation circulated online, publicly as well as in private groups, can interfere in democratic processes. Media and digital literacy skills empower citizens to take a more critical view of the content or information they encounter, helping to identify disinformation and misinformation and strengthen democratic participation.
- Support for professional journalism and media plays an important part in efforts to address disinformation, including commitment to establish journalistic norms.
- Media and digital literacy education to increase awareness about safety online are particularly important for more vulnerable individuals and communities. Efforts, however, need to be sensitive to the needs of particular groups. The approach for young people and older generations, for example, needs to correspond to their usage patterns.
- Given the technical limitations of the domain name system (DNS) to remedy specific content issues, continued stakeholder dialogue should clarify when, in what situations and on what types of abuses
the DNS may be used to remedy specific content problems, and to strengthen due-process towards ensuring an open, accessible and safe internet for all.

- Encryption helps users to achieve safety, privacy and freedom of speech, and plays a key role in building a free, open, safe and democratic Internet.
Addressing Advanced Technologies, including AI

- IGF could be used as a platform for developing cooperation mechanisms on artificial intelligence. A policy network on artificial intelligence could be considered for the upcoming work streams in order to review the implementation of different principles with appropriate tools and metrics.

Human-centric AI

- AI should be designed in a way that respects the rule of law, human rights, democratic values and diversity, and includes appropriate safeguards. It should benefit people and the planet by driving inclusive growth, sustainable development and well-being. While there are some existing principles on artificial intelligence, these are mostly soft laws at present. A global agreement cannot be achieved in one straightforward process. The development of meaningful global standards will require participation of the Global South and inputs from regional initiatives.

- AI should be truly human-centred, reflecting the voices of all. Oversight and enforcement mechanisms should follow principles and rules, with AI actors being held accountable for any damage caused. This is crucial for upholding the rights of affected and vulnerable individuals.

- AI continuously impacts lives – and societies need to adjust to the transformation it engenders with a new cooperation framework and governance model. Building a human-centred intelligent society requires the full cooperation of government, enterprises, social organisations and academia.

- The assumption that technology is a great equaliser is flawed. Technologies often amplify inequalities and cause harm to gender and sexual minorities, people with disabilities, and people from other marginalised communities. Machine learning technologies are often designed by a homogenous group of developers and make use of unrepresentative or biased data. Missing data should also be included in the analysis to come to meaningful conclusions.

- Stakeholder collaboration is necessary as societies grapple with managing AI deployment and the rapid evolution of machine-learning. Ongoing human control remains essential, to ensure that algorithms do not bring about outcomes that are out of our control. Breaking down silos between engineers and policy experts is critical to achieving this.

Trust, security and privacy

- Regulatory frameworks should provide a set of principles for social media platforms to fulfil their due diligence obligations regarding the management of content that damages democracy and human rights. Frameworks should contribute to the global conversation on online content moderation to empower users, including the most vulnerable groups and users of minority languages.

- AI facilitates the constant observation and analysis of data in order to personalise and target content and advertising. The resulting personalised online experiences risk disaggregating online information spaces and limit individuals’ exposure to diversity of information. Lack of information pluralism can
foster manipulation and deception – furthering inequalities, undermining democratic debates, and potentially enabling digital authoritarianism, hatred and violence.

- There is still no consensus yet on the technical, social, and ethical feasibility of using artificial intelligence to infer peoples' emotions. Systems that seek to achieve emotion recognition are becoming more detailed and fine-grained. Emerging technologies like affective computing, which studies how computers may recognise, interpret and simulate human affectations, need ethical assessment. It is important to respect and reflect the different institutional and cultural backgrounds of diverse countries and communities, while respecting inclusivity and conducting international comparison and cooperation in the area of artificial intelligence. Stakeholders from technical and non-technical communities need to exchange expertise and work together transparently to develop general principles that are sufficiently flexible to be applied in diverse contexts and foster trust in the AI systems of today and tomorrow.

- Transparency in the operation and reporting of algorithmic systems is essential for human rights. For some people, knowing this could be a matter of life and death.

**Content moderation and AI**

- Content governance by online platforms plays a significant role in shaping and arbitrating political and public discourse, including issues that affect both individual human rights and collective rights including social, economic and cultural rights and those to global peace and security. It is essential that policies and their enforcement are in line with international human rights standards.

- Artificial intelligence and machine-learning technologies are already being used to decide what content is removed, what is prioritised and to whom it is disseminated. These tools are often deployed with little or no transparency, accountability or public oversight. The decisions that are taken by them directly influence individuals’ right to seek, impart and receive information – and ultimately, their opinions – as well as affecting other rights.

- Many of the unintended consequences of automated content moderation become particularly detrimental in times of conflict or crisis, when they may silence critical voices online at a time when those voices and the safety of those with critical perspectives are essential. The same technologies can be used to surveil critical voices, to promote violent agendas and in other ways that infringe human rights.

- Technical standards cover a wide range of digital technologies and related infrastructures, services, protocols, applications, and devices that have enormous impacts on human rights. Yet the technical standard-setting processes within standards development organisations do not fully take into consideration human rights concerns. These processes are often opaque, complex, and resource-heavy for civil society and other stakeholders to access and follow systematically.