

# ICC BASIS Input to the Global Digital Compact

# 1. Connect all people to the internet, including all schools

### a) Core Principles

Delivering universal meaningful connectivity requires effective action on all three layers of the ICT ecosystem: accessible and affordable infrastructure and devices; appropriate applications and services built upon the infrastructure; and user ability to use a device and understand the features of these applications and services. As stated in the ICC White Paper on Delivering Universal Meaningful Connectivity this would require policymaking grounded on two basic principles:

- 1. Policy and regulatory mechanisms should promote the value of the entire communications and digital services ecosystem.
- 2. Policies should be non-discriminatory, technology-neutral, and supportive of innovative business models and the development and deployment of a wide range of technologies, standards, and system architectures.

#### b) Key Commitment/ Pledges/ Actions

Grounded in these principles, we note the following three priority areas where policy action should be taken:

- Facilitate investment across the entire digital value chain Policies should foster investment, competition, and innovation in the development and deployment of:
  - broadband services and connectivity devices, with the aim of expanding affordable access and end-user choice for broadband connectivity
  - content that helps drive and sustain adoption, including through expanded e-government services;
  - digital literacy and skills development, while also facilitating and supporting multisectoral initiatives that meet these objectives.

#### 2. Effectively manage spectrum

Allocation and licensing of spectrum should be transparent, fair, economically efficient, technology-neutral, and aimed at ensuring the availability of sufficient broadband-capable spectrum. Unlicensed, shared, and secondary uses of spectrum should be facilitated, and operators should be incentivised to use spectrum efficiently.

When targeting remote and rural areas, policies should aim at reducing cost of deploying broadband access, through easing licensing and permit processes, providing access to sufficient spectrum, including licensed spectrum at reasonable cost and unlicensed spectrum to support alternative technology approaches.

Two ways to enable more connectivity in rural and remote areas are putting in place non-discriminatory frameworks for providing access to low-cost licensed spectrum, preferentially at lower frequency bands which provide greater coverage, and providing greater access to unlicensed spectrum where it can support low-cost technologies in unserved or underserved areas.

## 3. Ground policies in evidence and data

Policymaking and regulation should be evidence-based, transparent, inclusive of all interested stakeholders, and aimed at improving the ease and predictability of doing business.

When targeting remote and rural areas, policymakers should strongly consider the increased complexity of delivering connectivity, and provide specific, adapted, flexible and non-discriminatory policy solutions in these areas.

Private investments and public funding mechanisms alike should be informed by accurate information and reliable data, including coverage and usage data, but also satellite images, census data and other relevant information that combined can provide detailed understanding ahead of decisions taken on where and how to deploy networks.

We also recall the <u>multistakeholder joint statement</u> presented to the 2021 High-Level Digital Debate of the UN General Assembly on Connectivity and Digital Cooperation that introduced principles for a People-Centered Approach to Achieve Meaningful Connectivity.

The Global Digital Compact should reiterate all member states' shared commitment to bridging both the coverage and usage gaps and bringing meaningful connectivity to all populations everywhere. The Compact should recognize the efforts of all stakeholders and encourage flexible and forward-looking policy and regulatory approaches that enable investments across the entire digital value chain, facilitate the effective management of spectrum and are grounded in evidence and data.

# 2. Avoid internet fragmentation

### a) Core Principles

The open, interconnected and interoperable Internet is a generally recognized principle and objective that is increasingly put at risk and undermined due to unintended consequences of technical, legislative, regulatory and policy developments that have an impact at any of the layers of the Internet.

- Technical / backbone layer: whereby conditions in the underlying technical infrastructure impede the ability of systems to fully interoperate;
- Network / access layer: whereby conditions at the physical, network, transport layers prevent proper functioning of the Internet and/or hinder meaningful connectivity;
- Application / content layer: whereby policies and actions constrain or prevent certain uses
  of the Internet to create, distribute or access information.

Concerned of these risks, ICC joined a coalition of civil society and industry stakeholders in setting out the following principles for an open, interconnected and interoperable Internet:

- 1. **Protect and promote human rights**, ensuring that the work of the UN and all its agencies continues to be anchored in the values and obligations of the UN Charter and the Universal Declaration of Human Rights and the UN Guiding Principles on Business and Human Rights.
- 2. **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.
- 3. 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 SDGs. The digital economy also depends upon the free flow of information, and ensuring compatibility across a diverse set of laws and regulations is essential in this regard.
- 4. Advocate for efforts to address the root causes of Internet fragmentation. Laws that fail to take into account the architecture of the Internet and place barriers to global connectivity contribute towards a more fragmented Internet. Such laws mainly focus on the deprivation of rights such as privacy, data protection and free expression, which undergirds many fragmentation initiatives. Promoting these rights on a global basis can defend against the forces of fragmentation.
- 5. Encourage cooperation to promote security and increase trust on the Internet. The implementation of international best practices is essential in addressing security threats and reducing vulnerabilities. To operationalise these, cooperation is needed among different stakeholders to ensure that these security principles do not inadvertently limit the global, open nature of the Internet.
- 6. Promote efforts to expand meaningful connectivity to the Internet. 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 and freedoms as well as economic, social and educational benefits. To be able to do this, regular, affordable, and secure broadband access on an appropriate device is critical. Access must be coupled with meaningful use of the Internet, which is enabled by

- digital literacy, trust, and online environments free from harassment, discrimination and violence, among others.
- 7. Commit to preserve and strengthen the multistakeholder model particularly by 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 (IGF), are further strengthened with appropriate human resources and funding. Meaningful participation of interested and informed stakeholders is essential to ensure that outcomes are both effective and accepted. It is particularly important to ensure the meaningful participation of stakeholders from the global South and other typically under-represented groups in global public policymaking pertaining to the Internet, including women.

### b) Key Commitment/ Pledges/ Actions

An open, stable and trusted Internet is vital for business operations worldwide and the effective functioning of public services such as education, health care or various government services. Technical, legislative, regulatory and policy developments threatening the open, interconnected and interoperable nature of the Internet also risk losing its associated benefits to social and economic development, while also harming human rights.

ICC BASIS is a strong supporter of the formation of the Internet Governance Forum Policy Network on Internet Fragmentation. This multistakeholder coalition aims to offer a systematic and comprehensive framework to define Internet fragmentation, its intended and unintended causes, and its potential effects; to collect and analyze case studies to fine-tune and complement this framework and to establish shared principles, recommendations or codes of conduct that prevent fragmentation and preserve the open, interconnected and interoperable nature of the Internet.

The Global Digital Compact should reiterate all member states' shared commitment to keeping the Internet whole, open, interconnected and interoperable.

The Compact should recognize the efforts of the Internet Governance Forum Policy Network on Internet Fragmentation to understand, map and bring recommendations to counter measures that might fragment the Internet at any of its technical, network or content layers.

### 3. Protect data

#### a) Core Principles

Cross-border data flows are at the heart of the world's economy, as companies rely on such flows to conduct their day-to-day business with customers and partners, innovate in their business and operations, and compete more effectively, in sectors as diverse as agriculture, healthcare, manufacturing and banking.

The processing and transfer of both personal and non-personal data are integral to many of these exchanges, making trust a vital element for resilient and sustainable economic growth. This is why ICC strongly supported the 2021 G7 Trade Ministers' Digital Trade Principles that aim to enable open digital markets; data free flow with trust; safeguards for workers, consumers, and businesses; digital trading systems; as well as fair and inclusive global governance. However, trust in international data flows is being eroded over concerns that government demands to access data may conflict with universal human rights and freedoms, including privacy rights, or cause concerns and conflicts with domestic laws when such access transcends borders.

These increased concerns and reduced trust have led to uncertainty that may discourage individuals,' businesses,' and even governments' participation in a global economy, and can negatively impact inclusive and resilient economic growth. Cooperation between governments and stakeholders, including business and multilateral organizations, is essential to develop interoperable policy frameworks that would facilitate cross-border data flows and enable data to be exchanged and used in a trusted manner. Efforts to define principles and safeguards for government access to personal data held by the private sector are urgently needed to provide a firm foundation for data-

free-flow-with-trust. The <u>ICC White Paper on Trusted Government Access to Personal Data Held by the Private Sector</u> presents a set of 8 draft principles in this regard:

<u>Principle #1 – Appropriate Legal Bases with Meaningful Opportunities for Stakeholder Input:</u> The laws, rules, and international agreements that allow for government access to personal data should be clear, comprehensive, and developed through transparent processes with meaningful opportunities for stakeholder input.

<u>Principle #2 – Legitimate Aims of Surveillance with Safeguards to Prohibit Unfair Treatment</u>: The purpose and reach of government access laws should be proportionate to meet defined public safety and national security needs. Authorities should not be employed to acquire commercial advantage or data held by foreign governments or the public sector.

The authorities should also include safeguards to prohibit unfair and discriminatory treatment. They should not allow the suppression of dissent or free expression, or target individuals based on race, ethnicity, religion, disability, sexual orientation, gender, or gender identity.

<u>Principle #3 – Requirements for Approval Commensurate with Privacy Intrusion</u>: The level of approval required for government access should be commensurate with degree of interference with privacy and other rights and freedoms, with prior judicial approval for any significant interference. Except in cases of true emergencies, criminal demands seeking intrusive personal data should be predicated on prior independent review.

<u>Principle #4 – Appropriate Protections for Handling Personal Data</u>: Governments must require strict and transparent data minimization, dissemination, and retention limits when they seek access to personal data of both citizens and foreign persons.

<u>Principle #5 – Transparency of Government Demands for Access</u>: The need for transparency extends to the legal framework allowing for government access; the publication of both government and service provider transparency reports that include statistical information on government demands, including national security demands in the aggregate; and the importance of prior user notice. The public has a right to know how, when, and why governments seek access to their data. Absent narrow circumstances, individuals and organizations should be allowed prior notice regarding law enforcement requests for their personal data.

<u>Principle #6 – Independent Oversight of Access Authorities</u>: All government access authorities should be subject to independent oversight. Any non-compliance with surveillance authorities should be both publicly reported and remedied.

<u>Principle #7 – Mechanisms Provided for Effective Redress</u>: Individuals, organizations, and providers impacted by a government access demand should have clear redress mechanisms through which to challenge unlawful or inappropriate demands in front of an independent authority, and remedies must be commensurate with the degree of injury.

<u>Principle #8 – Avoidance and Accounting for Conflicts of law</u>: In today's interconnected digital economy, government access laws must account for the fact that data is truly global and may be subject to the laws of multiple jurisdictions. International agreements should advance frameworks that minimize conflicts of law, and legal bases must include mechanisms to raise conflicts of law so providers are not forced to violate one country's laws to comply with another's.

In addition, government access policies should consider:

- Prohibition on excessive costs and burdens placed on providers: Government requests should not impose significant costs or burdens on providers, including data retention obligations unrelated to a business purpose.
- Intermediary liability: Providers should not be held liable for complying in good faith with legal obligations of jurisdictions in which they operate.

#### b) Key Commitment/ Pledges/ Actions

Businesses are committed to the protection of personal data, including when it is transferred across borders. It is incumbent upon companies to directly and comprehensively implement their legal obligations to protect privacy and security of data, across the entire processing lifecycle or locations of processing.

Governments should therefore assure that their policy and regulatory environments are up to date and reflect best practice regarding high levels of privacy and security protection. Lack of interoperability across the policy and regulatory environments can create needless administrative burdens and compliance inconsistencies across jurisdictions. Furthermore, as privacy is both subjective to the data subject and tied to the cultural and legal context of the jurisdiction, harmonisation can be difficult to achieve.

Therefore, there is a clear and urgent need to enhance cooperation on data governance, data protection and identifying opportunities to overcome differences, explore commonalities in regulatory approaches and promote interoperability. Such work should not diminish any jurisdiction's protection or aim for the lowest common denominator of privacy standards, but rather to find ways of avoiding duplicative compliance requirements and needless administrative burdens, while assuring adequate levels of protection.

The Global Digital Compact should recognize that establishing trust and minimising disruptions in data flows are fundamental to reaping the benefits of digitalisation. The Compact should call for unjustified obstacles to cross-border data flows to be removed, while continuing to address privacy, data protection, the protection of intellectual property rights, or security. The Compact should encourage global cooperation and interoperability across policy and regulatory systems on data governance matters.

# 4. Apply human rights online

#### a) Core Principles

Rights that people have offline must also be protected online, in accordance with the rule of law and international human rights legal obligations. Freedom of expression and the right to seek, receive and impart information in a safe environment are essential to protect the Internet's ability to catalyse development goals. Restrictions on freedom of expression and access to arts and culture using communications services and the Internet will diminish their usefulness, dampen the exchange of ideas, undermine public accountability, and reduce innovation and commercial opportunities.

#### b) Key Commitment/ Pledges/ Actions

In order to safeguard human rights and promote freedom of expression and access to arts and culture, policies should:

- Be consistent with international human rights obligations and trade laws to ensure compliance requirements, including those on privacy and security, are not conflicting with established global commitments.
- 2. Respect the rights of others and the rule of law.
- 3. Enable the free flow of information and the cross-border data flows that support it.
- 4. Be consistent with international treaties:

The right to free expression or access to arts and culture is not without limit, but should only be limited when necessary to enforce rules of law consistent with international treaties, such as protecting the rights of others, and any such restriction should be based in transparent laws and regulations. Decisions on Internet governance and policy issues on all levels should be consistent with international human rights.

The Global Digital Compact should reiterate governments' shared commitment to human rights and fundamental freedoms and recognize that rights people have offline must be equally protected online.

# 6. Regulation of artificial intelligence

### a) Core Principles

ICC is a strong supporter of the OECD Principles on Artificial Intelligence which promote artificial intelligence (AI) that is innovative and trustworthy and that respects human rights and democratic values. These value-based principles refer to:

- Inclusive growth, sustainable development and well-being: Stakeholders should proactively
  engage in responsible stewardship of trustworthy AI in pursuit of beneficial outcomes for people
  and the planet such as augmenting human capabilities and enhancing creativity, advancing
  inclusion of underrepresented populations, reducing economic, social, gender and other
  inequalities, and protecting natural environments, thus invigorating inclusive growth,
  sustainable development and well-being.
- 2. Human-centred values and fairness: Al actors should respect the rule of law, human rights and democratic values as freedom, dignity and autonomy, privacy and data protection, non-discrimination and equality, diversity, fairness, social justice, and internationally recognised labour rights. To this end, Al actors should implement mechanisms and safeguards, such as capacity for human determination, that are appropriate to the context and consistent with the state of art.
- 3. Transparency and explainability:

Al Actors should commit to transparency and responsible disclosure regarding Al systems. To this end, they should provide meaningful information, appropriate to the context, and consistent with the state of art:

- to foster a general understanding of Al systems,
- to make stakeholders aware of their interactions with Al systems, including in the workplace,
- to enable those affected by an Al system to understand the outcome, and,
- to enable those adversely affected by an Al system to challenge its outcome based on plain and easy-to-understand information on the factors, and the logic that served as the basis for the prediction, recommendation or decision.
- 4. Robustness, security and safety of Al systems:
  - Al systems should be robust, secure and safe throughout their entire lifecycle so that, in conditions of normal use, foreseeable use or misuse, or other adverse conditions, they function appropriately and do not pose unreasonable safety risk.
  - To this end, Al actors should ensure traceability, including in relation to datasets, processes and decisions made during the Al system lifecycle, to enable analysis of the Al system's outcomes and responses to inquiry, appropriate to the context and consistent with the state of art.
  - Al actors should, based on their roles, the context, and their ability to act, apply a systematic risk management approach to each phase of the Al system lifecycle on a continuous basis to address risks related to Al systems, including privacy, digital security, safety and bias.
- 5. Accountability: Al actors should be accountable for the proper functioning of Al systems and for the respect of the above principles, based on their roles, the context, and consistent with the state of art.

#### b) Key Commitment/ Pledges/ Actions

To complement these principles, the OECD also proposed recommendations to aid their implementation through national policies and international co-operation, with special attention to small and medium-sized enterprises (SMEs).

ICC builds on OECD Artificial Intelligence recommendations for policy makers made by the OECD Al Policy Observatory:

- 1. Investing in AI research and development
  - a) Governments should consider long-term public investment, and encourage private investment, in research and development, including interdisciplinary efforts, to spur innovation in trustworthy AI that focuses on challenging technical issues and on AI-related social, legal and ethical implications and policy issues.
  - b) Governments should also consider public investment and encourage private investment in open datasets that are representative and respect privacy and data protection to support

an environment for AI research and development that is free of inappropriate bias and to improve interoperability and use of standards.

- 2. Fostering a digital ecosystem for Al
  - Governments should foster the development of, and access to, a digital ecosystem for trustworthy Al. Such an ecosystem includes in particular digital technologies and infrastructure, and mechanisms for sharing Al knowledge, as appropriate. In this regard, governments should consider promoting mechanisms, such as data trusts, to support the safe, fair, legal and ethical sharing of data.
- 3. Shaping an enabling policy environment for Al
  - a) Governments should promote a policy environment that supports an agile transition from the research and development stage to the deployment and operation stage for trustworthy Al systems. To this effect, they should consider using experimentation to provide a controlled environment in which Al systems can be tested, and scaled-up, as appropriate.
  - b) Governments should review and adapt, as appropriate, their policy and regulatory frameworks and assessment mechanisms as they apply to AI systems to encourage innovation and competition for trustworthy AI.
- 4. Building human capacity and preparing for labour market transformation
  - a) Governments should work closely with stakeholders to prepare for the transformation of the world of work and of society. They should empower people to effectively use and interact with Al systems across the breadth of applications, including by equipping them with the necessary skills.
  - b) Governments should take steps, including through social dialogue, to ensure a fair transition for workers as Al is deployed, such as through training programmes along the working life, support for those affected by displacement, and access to new opportunities in the labour market.
  - c) Governments should also work closely with stakeholders to promote the responsible use of Al at work, to enhance the safety of workers and the quality of jobs, to foster entrepreneurship and productivity, and aim to ensure that the benefits from Al are broadly and fairly shared.
- 5. International co-operation for trustworthy Al
  - a) Governments, including developing countries and stakeholders, should actively co-operate to advance these principles and to progress on responsible stewardship of trustworthy Al.
  - b) Governments should work together in the OECD and other global and regional fora to foster the sharing of Al knowledge, as appropriate. They should encourage international, cross-sectoral and open multi-stakeholder initiatives to garner long-term expertise on Al.
  - c) Governments should promote the development of multi-stakeholder, consensus-driven global technical standards for interoperable and trustworthy Al.
  - d) Governments should also encourage the development, and their own use, of internationally comparable metrics to measure Al research, development and deployment, and gather the evidence base to assess progress in the implementation of these principles.

The Global Digital Compact should recognize ongoing work on establishing common principles for trustworthy AI, such as the work carried out by the OECD and since endorsed by the G20. The Compact should promote their further endorsement and uptake across the globe, as well as cooperation for their implementation.

# 8. Other areas (please specify):

Specify area:

Multistakeholder governance

#### a) Core Principles

The very nature of the global Internet necessitates an effective multistakeholder governance model to be at its core. This includes continued efforts by all stakeholders (individually and collectively, including private sector led, multistakeholder and intergovernmental) to address Internet-related issues and the promotion of greater cooperation among organisations. Such cooperation should be

guided by the objectives of information sharing, raising awareness and where appropriate, coherence among work programmes and collaboration.

A governance model fit to promote this culture of cooperation and coordinate activities to support it, must be:

- Multistakeholder: all relevant stakeholders (governments, business, technical community, academia, civil society) should participate, engage, and contribute to the discussions and decision-making.
- Bottom-up and distributed: an open and inclusive participation model fosters not only legitimacy and credibility, but also is flexible to rapidly adapt to changing technologies and issues and avoid unintended consequences.
- Transparent: decision-making processes should be consensus-based, clearly indicating how decisions are made and how multistakeholder input is reflected in such decisions.

The strength of such a mechanism lies not only in its open and inclusive participation model, and the legitimacy and credibility that it fosters, but also in its flexibility to rapidly adapt to changing technologies and issues.

Multistakeholder cooperation along these principles is indispensable for the realization of the objectives outlined in the UN Secretary-General's report on Our Common Agenda to deliver universal meaningful connectivity, avoid internet fragmentation, ensure data free flows with trust; protect human rights online, and promote trustworthy artificial intelligence, and therefoe should be prominently featured in the Global Digital Compact.

#### b) Key Commitment/ Pledges/ Actions

The Internet Governance Forum (IGF) embodies the above-mentioned principles and characteristics of multistakeholder cooperation and stands as the UN's only bottom-up multistakeholder mechanism serving as a pioneering example of cooperation among Internet governance stakeholders since its inception.

The IGF's invaluable feature as a venue for discussion and non-binding outcomes provides a "safe place" for stakeholders to test new ideas and unveil potential solutions. All participants benefit from an exchange of different viewpoints. With its emphasis on inclusiveness, the IGF also has enabled under-represented stakeholders from developing and least developed countries as well as a new generation of youth to engage in Internet governance discussions.

ICC and its members have been long-time supporters of the IGF, benefitting from the free exchange of ideas and informal relationship-building this Forum provides, rather than being tied up in extensive negotiation of specific textual outcomes. This has enabled thoughtful discussion and dissemination of best practices for the express purpose of enabling more countries to realize the economic and societal fruits of digital transformation.

In its nearly 20 years of operation, the IGF has not only advanced diverse and critical thinking but has also been successful at building community. The global IGF and its many national and regional initiatives (NRIs) have propagated cooperation and improved technical knowledge. They have brought together different stakeholders - nationally, regionally and globally - to share information and progress on their respective work, address policy matters in an open setting among a wide range of organizations and stakeholders, and produce intersessional output in the forms of best practice material and policy insights focused on a question or challenge.

Building on the importance of multistakeholderism, the Global Digital Compact should signal a commitment of member states to support the renewal of the IGF's mandate in 2025.