ICC |((BASIS

Your guide to business views on discussions at the Internet Governance Forum 2024

Global business strongly supports the multistakeholder model as a cornerstone of effective Internet governance and digital policy development. Through ICC BASIS, the International Chamber of Commerce represents private sector perspectives at the Internet Governance Forum (IGF), demonstrating how multistakeholder collaboration fuels initiatives to expand meaningful connectivity, safeguard a globally connected, unfragmented Internet, enable trusted cross-border data flows, enhance cybersecurity, combat cybercrime, and advance the responsible development of AI for good. Discover how ICC BASIS is championing these priorities at IGF 2024. Join the conversation on social media at @iccwbo on X and @International Chamber of Commerce on LinkedIn.

As the institutional representative of more than 45 million businesses in over 170 countries, the International Chamber of Commerce (ICC) considers Internet governance to be critical for the promotion of international trade, economic development, and innovation.
In today's digital economy, Internet governance has implications for businesses operating all over the world, regardless of location, sector or company size. Information and communication technologies (ICTs) and digital technologies present as an ally to drive economic and social progress and accelerate growth, at a time when the global community is falling short of reaching our commonly set goals for sustainable development. Coupling business innovation with enabling policy and regulatory measures for continued digitalisation is the catalyst needed to bring the 2030 Agenda back on track.

Global business firmly believes in the multistakeholder approach as an enabler of effective Internet governance and digital policy discussions. The reasons for this are manifold:

1. **Inclusivity and diverse perspectives:** The multistakeholder model brings together various stakeholders ensuring that multiple viewpoints and experiences are considered. This diversity leads to more comprehensive and balanced decision-making by considering the interests of different groups, including public policy objectives and business needs. This ensures that policies lead to evidence-based, inclusive and trusted outcomes.
2. **Enhanced legitimacy:** Multistakeholder processes strengthen the legitimacy and effectiveness of governance frameworks. When businesses participate alongside other stakeholders, it builds trust and credibility in the resulting policies, encouraging broader acceptance and adherence.
3. **Innovation through collaboration:** The multistakeholder approach encourages collaboration, enabling businesses to share knowledge, resources, and best practices with others. This sparks innovation and drives the development of new technologies and solutions.

4. **Flexibility and adaptability:** The multistakeholder approach allows for more responsive and adaptive governance structures in a constantly evolving digital landscape. Businesses can engage in discussions that quickly address emerging trends, challenges, and opportunities.

5. **International cooperation:** Challenges in the digital realm, such as cybersecurity threats and data privacy concerns, cross national borders. A multistakeholder approach facilitates global cooperation, enabling businesses to collaborate on shared solutions to common problems.

A well-governed and inclusive Internet is crucial for the sustainability and growth of the digital economy. Supporting the multistakeholder approach helps create a resilient digital environment that benefits all users and fosters development.

Our call to policymakers and stakeholders

Therefore, it is imperative to ensure that the multistakeholder approach is preserved and reflected across discussions that:

- expand connectivity and ensure meaningful access for everyone;
- promote a globally connected, stable, unfragmented Internet;
- enable data free flows with trust to support a truly global digital economy;
- increase efforts to strengthen cybersecurity and fight cybercrime; and
- foster the development of trustworthy artificial intelligence for good.

The IGF is the embodiment of the multistakeholder model. It offers a unique, open and inclusive setting for candid dialogue around issues, norms, principles and decision-making processes related to the use and evolution of the Internet and our digital world.

As the global community turns to the implementation of the commonly agreed Global Digital Compact and as we approach the 20-year review of the World Summit on the Information Society (WSIS+20), it is crucial to invest in the unique bottom-up governance model that the IGF offers. It is equally critical to continue to support its development as the only open, transparent and inclusive global space to address a wide range of issues pertaining to the governance of the digital world. The IGF already considers the policy matters these processes are tackling and is well placed to continue to do so.

To this end, business looks forward to contributing to the possible evolution of the IGF – and, specifically, to ensuring that this important mechanism is strengthened, agile and capable of supporting an inclusive and interdependent digital world.

ICC and its Business Action to Support the Information Society (BASIS) initiative work to ensure private sector views are represented at the IGF and all other forums where the future of the Internet and global digital policy cooperation are under consideration.

This guide concisely sets out business views on the key issues on Internet-related public policy matters to be discussed at IGF 2024, including connectivity, cybersecurity, data governance and artificial intelligence (AI).

We are looking forward to working with you!

Expanding meaningful connectivity

Private sector investment and innovation have transformed the Internet from an information exchange network to the platform for sustainable social and economic development we recognise it to be today. An open, stable, and trusted Internet is vital for business operations worldwide and a prerequisite to the effective functioning of public services such as education, health care or various government services. Sectors as wide-ranging as manufacturing, agriculture, logistics, and finance rely in varying degrees on ICTs and digital technologies. These technologies possess an unparalleled potential to **catalyse the achievement of the Sustainable Development Goals**, offering a transformative opportunity to bring the 2030 Agenda back on track and advance global development.

In order to reach their full potential, **ICTs must be accessible, affordable, and relevant** to the needs of everyone, every day, everywhere. Connecting the unconnected is not just about infrastructure and access to mobile, the Internet and new technologies. Meaningful connectivity requires a focus on adoption barriers, including the **establishment of an enabling environment** for the creation and availability of relevant content in local languages and addressing skills gaps.

Our call to policymakers and stakeholders

In pursuit of these goals and of human-centric, sustainable digitalisation, policymakers must improve their understanding of how ICTs work in practice, including knowledge of the ICT ecosystem, the roles of the various stakeholders and relevant policy issues. Frameworks that enable meaningful connectivity should be based on light-touch policy and regulatory approaches that consider the value of the entire communications and digital services ecosystem, encourage competition and the entry of new players into the ICT ecosystem to foster the emergence of innovative products, services, and business models.

Successful efforts to deliver universal meaningful connectivity must be grounded in evidence and data, enable the effective management of spectrum, and facilitate public and private investment across the entire digital value chain.

Find out more

[ICC White Paper on Delivering Universal Meaningful Connectivity](#)

[ICC Campaign on Digitalisation for People, Planet and Prosperity](#)

Promoting an unfragmented Internet

The unique potential of digital technologies as **catalysts of inclusive growth and sustainable development** can only be fully harnessed if the fundamental nature of the Internet as an open, interconnected, and interoperable network of networks is preserved.

Technical, legislative and policy developments – such as bans or restrictions on international data flows; techno-protectionist initiatives; interference with free expression, privacy, and/or encryption; and Internet shutdowns; among others – heighten the **risk that the Internet fragments into siloed parts**. These risks threaten the open, interconnected, and interoperable nature of the Internet, along with its associated benefits to social and economic development, while also harming human rights.

> **Our call to policymakers and stakeholders**
>
> All stakeholders must work together to promote policies that uphold the openness, interoperability, and resilience of the Internet that empowers all communities and drives shared progress.

Enabling trusted data flows for a global digital economy

Cross-border data flows **underpin every aspect of today's business** – cloud services, workplace collaboration, management of human resources, customer relationships and supply chains. They enable distance learning, telemedicine, the fight against cybercrime, fraud monitoring and prevention, investigation of counterfeit products, facilitate global trade and a broad range of other activities. The processing and transfer of both personal and non-personal data are integral to these exchanges, making **trust a vital element** for resilient and sustainable social-economic growth.

However, there is an increasing lack of trust in data and data-enabled technologies, due to concerns that policy objectives (privacy, security, consumer and human rights protection, or even industrial competitiveness) would be compromised when data moves abroad. Lack of trust can serve as the rationale for a growing number of compelled data localisation measures globally. They may result in increasingly **fragmented national approaches** to data governance and a growing number of restrictions that prohibit or considerably encumber cross-border data flows, and significantly **curb the economic and societal benefits** they enable.

> **Our call to policymakers and stakeholders**
>
> ICC urges governments to promote policies that facilitate the adoption of new technologies and the global movement of data that supports them. Policymakers should support open cross-border data flows, while also ensuring adequate privacy, security, and IP protections and that those protections are implemented in a manner that is transparent, non-discriminatory, and not a disguised restriction on trade.

One potential cause of eroding trust is the concern that government demands to access data may conflict with universal human rights and freedoms, including privacy rights, or cause conflicts with domestic laws when such access transcends borders. Principles and safeguards for government access to personal data held by the private sector are an essential first step in addressing cross-border data flows with trust. Such safeguards, based on existing best practices, can help protect individual rights, reduce conflicts of law, and ultimately serve as a foundation for enabling trusted global data flows when adopted by governments.

Trust is further strengthened through cooperation between governments and businesses on interoperable policy frameworks that facilitate cross-border data flows, enabling data to be exchanged and used in a trusted manner, thereby aiming for high privacy standards.

Find out more

[ICC White Paper on Trusted Government Access to Personal Data held by the Private Sector](#)

[ICC Policy Primer on Non-Personal Data](#)

Strengthening cybersecurity and fighting cybercrime

Cyberspace is an **intrinsic part** of **every country's development**, creating enormous opportunities and enabling everything from distance learning to economic and societal growth. However, its centrality to our everyday lives also introduces vulnerabilities, especially in low- and middle-income countries, as rapid digitalisation continuously challenges cyber resilience efforts. The Internet's borderless nature along with increased cyber-physical interdependencies pose complex policy and operational challenges that neither businesses nor governments can combat on their own.

As the backbone to every country's development, **safeguarding critical infrastructures and essential services** from evolving cyberthreats is a critical step to bolstering public safety, economic stability and national security.

Yet, **differing regulatory frameworks and definitions** continue to **pose challenges** to this endeavour. Addressing these requires **international cooperation** on baseline cybersecurity standards, coordinated threat mitigation, policy incentives for cybersecurity investment and strong public-private partnerships.

To counter rising cybersecurity risks, the multistakeholder community should embed cybersecurity capacity building within digital development, harmonise regulatory standards, and collaboratively define actionable goals to enhance online security. This would incentivise collaboration in closing digital divides, bolster resilience by fostering access to digital transformation, and enable the implementation of international law and norms to curtail malicious cyber activities.

Given the rapidly increasing growth of transnational cybercrime, global business welcomes the increasing efforts of the international community to address this. However, as governments consider ratifying the [UN International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes](#), ICC urges a careful evaluation of potential risks, including potential impacts to national security, unchecked data access and collection, reduced privacy protections, and adverse effects on investment in cybersecurity defense. Instead, ICC encourages support for existing international frameworks that balance effective cybercrime prevention, detection, and prosecution, with data protection, privacy and human rights safeguards, creating a more predictable environment for businesses and reducing the complexities of managing cross-border cyber incidents.

Find out more

[ICC Policy Primer on Cybersecurity](#)

[ICC Cybersecurity Issue Brief #1: Call for government action on cybersecurity](#)

[ICC Cybersecurity Issue Brief #2: Implementing norms and rules for responsible state behaviour in cyberspace and enhancing cooperation to counter cybercrime](#)

[ICC Cybersecurity Issue Brief #2 Annex: Substantive considerations on an international instrument on cybercrime](#)

[ICC Working Paper on protecting the cybersecurity of critical infrastructures and their supply chains](#)

[Global business urges governments to reject new international cybercrime treaty](#)

Fostering trustworthy AI for good

AI is a general-purpose technology that holds the potential to increase productivity and build cost-effective, **impactful solutions** across numerous sectors. It is perceived as a great transformer for both developed and developing economies, promising to enhance decision-making processes through the knowledge gained from applying analytics and machine learning to available data.

At the same time, the design, development and deployment of algorithmic systems and tools holds **challenges**, often surrounding the **role of humans, transparency**, and **inclusivity**. Recent advances, and the overwhelming popularity of user-friendly generative AI, have exponentially amplified its power to spur both beneficial and harmful change. As AI continues to evolve, it is essential to **strike a balance** between realising its **full potential** for socioeconomic development, while ensuring that it aligns with globally **shared values and principles** that foster equality, transparency, accountability, fairness, reliability, privacy and a human-centric approach.

Our call to policymakers and stakeholders

ICC advocates for a four-pillar approach to global AI governance, built on principles and codes of conduct, regulation, technical standards, and industry self-regulation. Effective AI governance must be anchored in this four-pillar structure, supported by the convergence of governance approaches and international cooperation. It should take a risk-based approach, addressing both high- and low-risk AI without imposing regulatory burdens that stifle innovation, while also recognising the diverse roles and responsibilities of stakeholders throughout the AI lifecycle.

Find out more

ICC Overarching narrative on artificial intelligence

About the International Chamber of Commerce

The International Chamber of Commerce (ICC) is the institutional representative of more than 45 million companies in over 170 countries. ICC's core mission is to make business work for everyone, every day, everywhere. Through a unique mix of advocacy, solutions and standard setting, we promote international trade, responsible business conduct and a global approach to regulation, in addition to providing market-leading dispute resolution services. Our members include many of the world's leading companies, SMEs, business associations and local chambers of commerce.

ICC ((

33-43 avenue du Président Wilson, 75116 Paris, France
T +33 (0)1 49 53 28 28   E icc@iccwbo.org
www.iccwbo.org   @iccwbo