Contribution for the Leadership Panel

Context

The Leadership Panel (LP) of the Internet Governance Forum (IGF) was created in 2022 by the United Nations Secretary-General Mr. António Guterres. One key element of the Terms of Reference of the LP is to provide strategic inputs and advice on the IGF and to promote the Forum and its outputs.

The LP actively supports a vision of strengthening the multistakeholder model in Internet governance processes. As part of their advice to strengthen the IGF they have, in dialogue with stakeholders, created a vision and a framework for the future Internet, "The Internet We Want" (IWW). IWW has been presented at the most recent IGF held in Kyoto, Japan, in October 2023, and the LP is eager to ensure that as many stakeholders as possible give input and feedback on the framework. The aim is to concretize the framework together with all stakeholders and complement it with measurable goals to facilitate the implementation of this shared vision.

The LP is most interested in hearing on what challenges or obstacles you see that might hinder the implementation of this vision to help us pinpoint priority areas for action and set

more concrete goals. You can find the consultation on this link, where you can share your comments under each of the IWW's five sections:

1. Whole and open;
2. Universal and inclusive;
3. Free-flowing and trustworthy;
4. Safe and secure; and
5. Rights-respecting.

Website: https://www.intgovforum.org/en/content/the-internet-we-want

Deadline for Submission, 1 March 2024

Sections

Section 1 – Whole and Open

A whole, open, free, globally connected, interoperable and stable Internet is vital for sustainable development, the functioning of digital societies and economies, for supporting business operations worldwide, and a prerequisite to the effective functioning of public services such as education, health care or various governmental services. When properly harnessed, information and communication technologies (ICT) and digital technologies are formidable engines of innovation, competitiveness development, sustainable economic growth, and instruments of social, cultural, and economic empowerment for all.

This unique potential can only be fully exploited if the fundamental nature of the Internet as an open, whole, interconnected, and interoperable network of networks is preserved. However, at present, there is a heightened risk that some potential policy or business decisions might fragment the Internet into siloed parts.

The potential fragmentation at either the technical, content or governance layers, threatens the open, whole, interconnected, and interoperable nature of the Internet, and its associated benefits to social and economic development, while also harming human rights.

We call on the stakeholders of the Internet to set goals to ensure that the internet stays whole, open, free, globally connected, interoperable, stable and unfragmented.

ICANN's Contribution to Section 1

Response from ICANN
The preservation of the Internet as an open, whole, interconnected, and interoperable network is integral not only for the Internet's technical functionality but also for supporting human rights and fostering social and economic development. The threat of fragmentation, be it through policy, technical, or governance means, challenges this vision and calls for a unified response.

Central to this response is the recognition of the technical community's pivotal role within the multistakeholder approach to Internet governance. The technical community, with its deep understanding of the Internet's infrastructure and operations, brings invaluable insights into ensuring the network's stability, security, and resilience. Their expertise is crucial in shaping the standards and policies that uphold the Internet's interoperability and openness, and in addressing emerging challenges in cybersecurity and the digital landscape.

Following the COVID-19 pandemic, there is a heightened need for policies that expand connectivity and ensure equitable access to the Internet. This need extends to embracing linguistic diversity and cultural inclusivity, as demonstrated by the expansion of Internationalized Domain Names, enabling a multitude of languages and scripts in domain names and email addresses.

Furthermore, the integration of Internet governance with respect for human rights, democracy, and the rule of law is vital. Strengthening cybersecurity and fostering a safe online environment are essential to build trust and protect users.

The contributions of the technical community are indispensable in these areas. Our expertise not only informs policy decisions but also ensures that technical advancements along with socioeconomic policy/regulation align with the broader goals of an inclusive, secure, and sustainable Internet. As such, all stakeholders' involvement in the multistakeholder process is key to developing comprehensive and effective Internet governance strategies.

Section 2 – Universal and Inclusive

Since its inception, the Internet has evolved 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 the effective functioning of a diverse array of services, as varied as agriculture, energy, healthcare, manufacturing, or education, continuously reimagining the way people interact with their peers, businesses, and

governments. However, despite the enormous progress in expanding connectivity in recent years, 2.7 billion people remain unconnected.

Connecting the unconnected and reconnecting the disconnected is not just about infrastructure and access to the Internet. Meaningful connectivity also requires focus on bridging the barriers to adoption, including creating and maintaining an enabling environment in which locally relevant, local language content is created, as well as adopting policies and tools designed to identify and address skills gaps. The enduring digital divide in access, application, and skills among and within countries emphasize the need for universal, affordable, and meaningful connectivity in order to reach the development potential of the Internet, ICTs, and digital technologies. Meaningful connectivity should also be secure, resilient and cost-effective.

In pursuit of these goals and of a human-centric, sustainable digitalization, all stakeholders 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 Internet connectivity should be based on light-touch ICT policy and regulations, encourage universal access through competition and the entry of new players into the ICT ecosystem to foster the emergence of innovative products, services, and business models. Policy and regulatory mechanisms should consider the value of the entire communications and digital services ecosystem. They should be non-discriminatory, technology-neutral, and supportive of innovative business models and the development of a wide range of technologies, standards, and system architectures. Successful efforts to deliver universal meaningful connectivity need to balance the needs of all stakeholders, should be grounded in evidence and data, should seek global harmonization in terms of interoperability and standards, should enable the effective management of spectrum between all stakeholders, and must facilitate investment across the entire digital value chain.

We call on the stakeholders of the Internet to set goals to move towards universal meaningful connectivity for everyone, everywhere, to encourage the uptake of new technologies at need, and to address skills gaps.

ICANN’s Contribution to Section 2

Response from ICANN

For the Internet to be truly universal and inclusive for billions of people globally, it needs to be able to support the different languages and scripts used across the world. This means that not only that communities should be able to manage multilingual content online but equally important that they are able to access this content in their languages and scripts.

Therefore, enabling domain names and email addresses in the different languages and scripts of the world has been of significant focus at ICANN.

Since the early 2000s, the ICANN community and organization have been actively engaged in developing and implementing guidelines, procedures, and policies, as well as applying standards, to enable the Internet's Domain Name System (DNS) in the different languages and scripts. In addition, ICANN has worked with the community to document rules for forming secure and usable domain names in 26 commonly used scripts that cover more than 350 commonly used languages. ICANN continues to work to support additional languages and scripts in the DNS. For example, ICANN is currently working with communities using the following scripts: Balinese, Javanese, Thaana, and Unified Canadian Aboriginal Syllabics.

Based on this work, the DNS has changed dramatically over the last decade in regard to the overall number of generic top-level domains (gTLDs), scripts and languages used, and character length. There are now more than 1,200 active gTLDs and country code top-level domains, which provide users more choice. More than 150 of these top-level domains (TLDs) are available in 37 different languages in 23 different scripts. These new TLDs provide greater consumer choice and can represent languages, cultures, brands, geographies, special interests, and more (e.g., .ไทย, .london, and .sport).

Many people around the world are still excluded from experiencing the full benefits of this growing and multilingual Internet simply because they are unable to use a valid domain name or email address in their language and script of choice. This is because many of the software applications do not accept these valid domain names and email addresses created using these new and multilingual TLDs. For example, a user cannot use an email address in a local language to register for an online social media app or an e-government service, domain names with these TLDs are not automatically converted into links that can be clicked to seamlessly traverse the Internet, or these domain names are not displayed correctly in local language form for small or medium enterprises to use them for marketing purposes.

Universal Acceptance (UA) of domain names and email addresses is now needed to enable users globally to experience the complete social and economic power of the growing Internet. Specifically, UA means that all domain names and email addresses work in all Internet-enabled applications, devices, and systems. Governments should implement procurement policies that require support for local language domain names and email addresses on government websites and applications, thereby improving citizens' access. Technology companies need to update their software design guidelines to include default support for local language domain names and email addresses in websites, applications, and email systems. University and educational institutions should incorporate universal acceptance concepts into their IT curricula. Finally, civil society is encouraged to raise awareness and advocate for the practical application of local language domain names and email addresses in communities.

ICANN has been working with its community to continue to make domain names in the different languages and scripts available for use by the communities globally. ICANN is also working with the community to raise awareness and encourage the adoption of UA. Current results show that around 10 percent of popular online websites support the acceptance of email addresses in local languages through their contact forms, while there is a 23 percent rate of support of email addresses in local languages in email servers deployed under gTLDs. So there is a continued need to raise this issue more broadly to all the stakeholders to make the Internet truly universal and completely inclusive. For more details, see https://icann.org/idn and https://icann.org/ua.

Section 3 – Free-flowing and Trustworthy

Cross-border data flows underpin many aspects of business today — cloud services, remote work, workplace collaboration, management of human resources, customer relationships and supply chains. They also underpin distance learning, telemedicine, the fight against cybercrime and child abuse online, fraud monitoring and prevention, investigation of counterfeit products, and a broad range of other activities. 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 and recovery.

However, there is an increasing lack of trust, or confidence, due to concerns that policy objectives—such as privacy, national security, consumer and human rights protection, access to data or even industrial competitiveness—would be compromised when data moves abroad. This lack of trust serves as the rationale for the adoption of an increasing number of data localisation and sovereignty measures, leading to fragmented national approaches to data governance and a growing number of restrictions that prohibit or considerably encumber cross-border data flows. Failure to address this lack of trust and to find an appropriate trust model risks impeding cross-border data flows, thereby limiting economies of scale and scope, driving inefficient, unsustainable investment, and restricting innovation.

Promoting policies that facilitate the adoption of applicable technologies and the global movement of data, including through governance models that allow for data-sharing for public good, is fundamental to harnessing their significant economic and social benefits. In particular, policymakers should support open cross-border data flows, while also assuring the protection of privacy, security, as well as intellectual property, and that those protections are implemented through a risk-based approach and in a manner that is transparent, non-discriminatory and in line with the principles of necessity and proportionality.

Trust is strengthened when governments adopt robust and comprehensive commitments to protect the rights and freedoms of individuals, including the fundamental right to privacy. In addition, cooperation between governments and stakeholders including business and multilateral organizations is needed to advocate for interoperable policy frameworks that would facilitate cross-border data flows, enabling data to be exchanged, shared, and used in a trusted manner, thereby aiming for high privacy standards.

We call on the stakeholders of the Internet to set goals to unlock the value of data flows for sustainable development of all and enshrine trust as the prerequisite for data sharing regimes, founded on the protection of data.

ICANN's Contribution to Section 3

ICANN does not have a contribution to this section.

Section 4 – Safe and Secure

Response from ICANN
Cyberspace is now an intrinsic part of every country's development, creating enormous opportunities and enabling economic and societal growth. At the same time, the indispensable nature of cyberspace in day-to-day human activities also generates growing vulnerabilities. Rapid digitalisation is testing the resilience of cyber infrastructures. The escalating vulnerabilities resulting from disparate states of cyber hygiene hinder the effectiveness of countermeasures against cyber attacks, threatening to thwart the potential economic impact of ICT and digital technologies.

The borderless nature of the Internet and the associated digital economy, the increased cyber-physical interdependency of IoT, and cybercrime paint a complex legal and operational picture for cybersecurity. A collective, collaborative multistakeholder approach is required to find meaningful ways and effective solutions to mitigate local, cross-border and global cybersecurity concerns.

To empower and protect societies from increased cybersecurity risks, the international multistakeholder community should explore practical ways to mainstream cybersecurity capacity building (CCB) into broader digital development efforts. This is also essential for building resilient societies and promoting a whole-of-society approach to dealing with threats emanating from cyberspace.

We call on the stakeholders of the Internet to set goals to establish and implement robust frameworks for high levels of cybersecurity, and strong recommendations for legal structures, practices, and cross-border cooperation to combat cybercrime.

ICANN's Contribution to Section 4

Response from ICANN
Cybersecurity and cyber-hygiene are critical elements that support trust on the Internet. The challenge for the world today is to be able to translate some complex cybersecurity concepts into simple concepts and practices that not only users need to adopt, but vendors also need to implement by default in applications and connected devices. Recognizing this has many facets; it must be broken into simple components to be tackled at different levels through multistakeholder principles.

Since ICANN's mission focuses on the Internet identifier systems that bring the global infrastructure together, we pay close attention and promote standards evolution that support cybersecurity and similar best-practice frameworks.

Internet standards such as DNS Security Extensions (adding authentication to DNS responses), DNS over HTTPS and DNS over Transport Layer Security (adding privacy to DNS data), and Resource Public Key Infrastructure (further securing the global address routing system) have been developed through multistakeholder processes and need to be implemented by operators globally. Through its capacity-building and community engagement programs, ICANN and its partners worldwide provide awareness and support to the operator community. These awareness efforts are also wrapped into supporting security frameworks such as Mutually Agreed Norms for Routing Security and Knowledge-sharing and Instantiation Norms for DNS and Naming Security.

The need to continue strengthening the multistakeholder effort to address the global cybersecurity challenge remains critical. There is no single stakeholder or approach that can effectively address the challenge.

5. Section 5 - Rights Respecting

Human rights must be respected online and offline. Governments are responsible to ensure that human rights are respected, protected, and promoted, while businesses and digital service providers are obliged to comply with all applicable laws and to respect human rights. Governments must refrain from Internet shutdowns. Any restriction of access to the Internet must be lawful, legitimate, necessary, proportional, and non-discriminatory.

All stakeholder groups have the responsibility to promote transparency, accountability, and human rights due diligence throughout the lifecycle of existing, new and emerging technologies. We recognize that certain behaviors have the potential to inflict significant

harm on our societies. Our vision for the Internet is one that safeguards us against such threats.

A human rights-based approach to Internet governance is required in order to realize the full benefits of the Internet for all, including the rights to education, to participation in public and cultural life or to access to information, as well as empowering businesses of all sizes. To that end, standards development organizations should introduce processes to ensure due consideration of human rights in their work, including by inviting participation of experts from all stakeholder communities.

We call on the stakeholders of the Internet to set goals to ensure a human rights-based approach to Internet governance, and to promote human rights in the digital space.

ICANN's Contribution to Section 5

Response from ICANN
In the evolving landscape of Internet governance, the imperative to uphold human rights stands at the core of creating a secure, accessible, and open Internet. Recognizing this, efforts are underway across various organizations, including within ICANN, to embed human rights considerations into Internet governance. This approach is paramount for ensuring that the Internet continues to be secure, and allow access for all users.

Recognizing that human rights are interrelated is essential so that all goals related to human rights impacts are realistic and require balancing perspectives and priorities. To this end, discussing potential human rights impacts as early as possible in developing policies and processes is the best practice.

ICANN's commitment to these principles is reflected in its ongoing initiatives to integrate human rights into its policies and operations. By fostering a dialogue among all stakeholders, including governments, businesses, civil society, and technical communities, we aim to promote a governance model that is transparent, accountable, and inclusive. Supporting this dialogue is essential because human rights are interdependent and often the ability to fulfill one right relies on the fulfillment of others. Additionally, no one right is superior to others. In order to balance human rights impacts with efficient and effective policy outcomes, it is essential to engage with human rights principles early in the process of generating and refining the procedures that are crucial for the functioning of the Internet.

Our goal is to ensure that the Internet not only supports but facilitates the access to information, participation in cultural and public life, and the empowerment of communities

worldwide. The collective engagement and commitment of all stakeholders are essential to achieving an Internet governance ecosystem that respects and promotes human rights.