Synthesis Document

Asia Pacific Regional Internet Governance Forum Brisbane 2023

Process

The Synthesis Document aims to document items of common interest relevant to Internet governance in the Asia Pacific region and has developed into one of the highlight innovations of the Asia Pacific Regional Internet Governance Forum (APrIGF) and inspired other national and regional initiatives to develop their own processes.

The 2023 Synthesis Document was drafted, synthesized and published by the 2023 Drafting Committee with the assistance of the APrIGF Secretariat.

Public input was sought during public input period I (21 August – 3 September), APrIGF conference Townhall sessions (29-30 August) and public input period II (22 – 28 September)

Comments were collected on the platform: https://comment.aprigf.asia during the public input periods.

2023 Drafting Committee

Lokendra Sharma, *Co-chair, Trust track lead*
Yien Chyn Tan, *Co-chair, Inclusion track lead*
Shradha Pandey, *Sustainability track lead*
Dr. N. Sudha Bhuvaneswari
Minkyoung Cho
Amrita Choudhury
Charlotte Fang Hendro
Uzair Farooqi
Waqas Hassan
Mohammad Ali Jauhar
Cherie Lagakali
Brian Mangi
Agita Pasaribu
Abdullah Qamar
Winston Roberts
Dr. Saima Nisar
Stella Anne Teoh Ming Hui

For full affiliation information, please see Appendix I

Table of Contents

Preamble

The Asia Pacific Regional Internet Governance Forum 2023 (APrIGF 2023) was held from 29-31 August in a hybrid format — virtually, and physically in Brisbane, Australia. Participants also joined from the nine local hubs[1] located across Bangladesh, India, Philippines, and Sri Lanka.

The overarching theme for APrIGF 2023 was *"Emerging Technologies - Is Asia Pacific Ready for the Next Phase of the Internet?"*[2]. Over the past few years, there has been a rapid increase in the adoption and development of emerging technologies in the Asia Pacific (APAC) region. Emerging technologies include Artificial Intelligence (AI), Augmented and Virtual Reality (AR/VR), Internet of Things (IoT), robotics, big data, 5G, blockchain, quantum computing, and others. More recently, ChatGPT and other AI applications have revolutionised chatbots, search engines, image/video generators, among others. These technologies could have significant impacts on the social, economic, and environmental future of the region, particularly in the context of uneven digitalisation and millions still unconnected. The central question throughout the APrIGF 2023 event was: what should the next phase of the Internet look like in the APAC region?

The main theme incorporated three high-level thematic tracks, namely "Access & Inclusion", "Trust", and "Sustainability". The use of high-level thematic tracks was to enable discussions on cross-cutting issues related to Internet Governance (IG) in the APAC region. This allows the APrIGF community to recognise and appreciate the complexity and interrelated nature of diverse IG issues and understand their significance at a policy level in all economies across the region.

As such, the APrIGF Multistakeholder Steering Group (MSG)[3] adopted a more flexible and all-encompassing approach since the APrIGF 2021 program. These high-level themes are designed to encompass various sub-topics under each track, and participants are encouraged to approach policy discussions creatively in an interdisciplinary and multidisciplinary manner.

As part of APrIGF 2023, a parliamentary track was held from 31 August–1 September. The parliamentary track gathered APAC government decision makers to discuss a range of Internet and digital issues, and to hold these conversations with other stakeholders such as the technical community and youth. Also, the 2023 Asia Pacific Youth Internet Forum, the 2023 Pacific Internet Governance Forum and the 2023 NetThing were co-located with the APrIGF 2023 in Brisbane, Australia.

[1] APrIGF 2023 Local Hubs: https://www.aprigf.au/localhubs
[2] APrIGF 2023 Overarching theme: https://ap.rigf.asia/news/2023/aprigf-2023-overarching-theme-emerging-technologies-is-asia-pacific-ready-for-the-next-phase-of-the-internet/
[3] APrIGF Multistakeholder Steering Group: https://ap.rigf.asia/msg/

Access and Inclusion

The principle of universal access and inclusivity advocates that no one should be disadvantaged on the basis of their background, location, gender, disability, religion, caste, class, or any other factors.

Meaningful and affordable access is still a big challenge in the Asia Pacific region, with millions still unconnected, especially from marginalised communities. There is a need for multistakeholder dialogue to focus on providing infrastructure and access to all, and to further enable the use of emerging technologies for socio-economic development.

Universal and meaningful access deserves further consideration, and not just limited to connectivity and infrastructure. Other aspects such as digital literacy and general access to information should be addressed. It is also important to adopt ways to measure access, and identify current methods to empirically measure, track, assess, and evaluate the benefits from increasing access and inclusivity.

With rapid development of emerging technologies, these technologies should provide an enabling platform for everyone to participate, raise their voices, and partake in the benefits.

No one left behind

There is vast uneven access and digitalisation discrepancies across the APAC region. Developed economies have progressed to widely adopt emerging technologies, while many developing economies are still struggling to get connected online due to factors such as a lack of infrastructure, digital literacy etc. Developed economies should consider providing support to developing economies, such as forming partnerships in building infrastructure and digital skilling, to address the gaps within the region.

In an increasingly interconnected society, lack of access to the Internet can tremendously impact daily life activities. For example, some organisations (e.g. banks) withdraw physical provision of services to push for web-based services, justifying closure of offices in small communities (and even in cities). Such decisions affect the daily operations and lives of communities.

There is a need to identify innovative approaches to connect the population in remote and geographically inaccessible areas. Technical (e.g. distance, remoteness) as well as adoption challenges (e.g. language, disability, literacy) need to be addressed.

In many areas with no Internet connectivity or weak mobile signal penetration, Community Radios serve as the medium of communication. In addition, Low Earth Orbit satellites are potential tools that provide cost-effective Internet access to remote and inaccessible regions. Such technologies help to bridge the communication divide, safeguard digital rights, as well as promote inclusivity and freedom of expression.

On the other hand, “inclusivity” would also consider the rights of certain communities on refusal to get connected online. Various factors could contribute to the refusal– for example, an Indonesian village had requested to be disconnected[4] to protect their community from negative impacts from accessing the Internet. Corresponding benefits or risks from these refusals should be assessed and discussed with these communities. Potential solutions include capacity building, education and better regulation to eliminate the negative effects from which these communities could suffer.

Digital transformation initiatives

If we consider that equitable access to information is a human right — that it is a necessity like food, clothing and shelter; that the Internet is now (or should be) a mainstream service — then universal and meaningful access must be available to all.

With the wide adoption of the Internet, digital transformation has been a core focus area for many economies in the APAC region. Although there are unique challenges to different economies, significant efforts have been put in place for building a digitally enabled environment. For instance, organisations such as the United National Development Program have been supportive in facilitating digital transformation in small island nations in the Pacific region.

Progressing digitally brings about various benefits; however, corresponding unintended consequences should also be considered. Potential concerns include widening the digital divide, increasing misinformation, and rising cybersecurity threats. Using digital identity systems as an example, measures (e.g. a civil registration system) should be developed to ensure sufficient data governance, data privacy and an appropriate justice framework.

Further collaborative efforts across the region and among different stakeholders are needed to ensure consistent progress towards a digital economy.

International Domain Names as a solution

The diversity of languages and scripts used in the APAC region is large, and many do not speak English or do not use English as their primary language. The language barrier is one of the key obstacles to the remaining unconnected population getting online. Internationalized Domain Names (IDNs) — domain names in local languages and scripts — will connect the next billion users to the Internet. IDNs will allow for a multilingual Internet, and users will be able to communicate online in their preferred languages/scripts.

Websites with content in local languages will be truly meaningful with corresponding domain names in local languages/scripts (i.e. website search will also be in the local language/script). In

[4] Syakriah, Ardila. "The Indonesian village that wants to cut off the Internet". *The Guardian*. 28 July 2023. https://www.theguardian.com/world/2023/jul/28/the-village-that-wants-to-cut-off-the-Internet

addition, IDNs will also allow for cultural preservation, retaining the roots and languages/scripts of many peoples (e.g. there are over 100 languages/dialects spoken by Aborigines in Australia; Indonesia has a wide range of scripts used across the country). Further, there is potential for development of IDNs use through voice mechanism, shifting away from only relying on the use of texts and creating opportunities to provide access to populations who are unable to type.

In the past 20 years, the multistakeholder community has moved ahead with efforts on addressing challenges on the use of IDNs. Two key aspects worked on were technology (setting technical standards and specifications) and policies (discussions on security issues such as homoglyphs). Progress on both aspects facilitates IDNs adoption.

More recently, the community is working together to ensure Universal Acceptance (UA), allowing for all domain names to be accepted and functioning across all systems. At the current stage, the main focus will be on increasing awareness and demand for IDNs.

Educating on the importance of IDNs to enhance digital inclusion is key. The Internet is only truly inclusive if it offers content, websites, interfaces, systems and other features in languages other than English. With the adoption of emerging technologies, there is a risk of biased machine learning (such as large language models with artificial intelligence based applications) as most content online is still in English and not truly reflective of the languages/scripts used by the global population.

Governments as key players to enhance Access and Inclusion

Governments lead the way

Governments play a key role in leading efforts towards enhancing access and inclusion. Governments need to ensure digital public services are accessible to all. Accessibility level should also be measured through a standards-based approach. Referring to standard-setting bodies such as the Assistive Technology Development Organisation (ATDO)[5], international standards and best practices should be adopted and enforced by governments.

Certain direct measures to enable access, especially for marginalised groups, can also be taken. One such example is the Indira Gandhi Smartphone Scheme in Rajasthan, India, where smartphones were distributed to women and students.

Procuring accessible ICT equipment

It would be useful for governments' procurement policies to mandate inclusive and accessibility features for all purchased Information and Communications Technology (ICT) systems, equipment, and services. When governments adopt such accessibility-centric policies, it can

[5] Assistive Technology Development Organisation: http://www.atdo.jp

create a ripple effect on the rest of the technology sector to adopt inclusive design principles and to add value to their products.

For instance, UA-readiness and accessibility for persons with disability (PWDs) requirements should be included in the policies. These accessibility features would encourage the use of IDNs (leading to increased connected users), as well as create a huge impact on providing assistive services to PWDs. As an example, the 'Be Safe'[6] project in Sri Lanka aims to help the female disability community through helpline, text and voice services. Such features should be integrated with official disaster management systems to enhance their impact at the national level.

Identifying emerging technologies' value

Governments should also take an active role in assessing impact of new technology deployment, and determine which ones could potentially enhance access and inclusion.

Maintaining open information flow

While it is important for governments to focus on protection against online abuse activities, it is essential to balance these efforts (and corresponding national legislations) against equitable access to information and freedom of expression. Certain mitigation actions such as Internet shutdowns could cause asymmetry in information flows, restricting access to certain populations.

Providing access to information through public education institutions

Another critical aspect in enhancing inclusion and access to information is the presence of an effective library service, to which the whole community has access. Public libraries, or other similar organisations providing information to the public, are usually supported financially and administratively by local governments. Also, these organisations' roles are usually defined by legislation through policies developed in consultation with communities.

Hence, governments play a key role in ensuring schools, libraries or similar organisations continue to provide such critical services, and are accessible to the public. This also includes procuring equipment that provide access at low cost (or no cost), instructions in local languages, use of assistive technology to encourage use of marginalised communities.

Achieving SDGs

All economies should work on their Voluntary National Reviews (VNR) for documenting progress towards achieving Sustainable Development Goals (SDGs). Specifically, VNRs should outline the role of the Internet towards achieving SDGs, and include information on progress for overcoming the digital divide, promoting digital literacy, and other similar efforts.

[6] "Be Safe project" https://forms.for.asia/proposal/?proposalform=NjQ1MzQ4MWNhMjk2ZS8vMjMvLzEyNDYvLzA=

Public-private partnerships

In addition to governments leading the way, private sector organisations (e.g. businesses, financial actors) can also contribute significantly to enhancing access and inclusivity. Public-private partnerships are needed to further such developments.

As an example, the New Zealand National Library (part of a government department) and the national professional library association collaborated during the COVID-19 pandemic to ensure ongoing provision of essential services such as access to information and digital skilling for users. With fixed-term funding from the government, public libraries were able to remain open during the pandemic, and adapted their provided services during the "lockdown period".

Focusing on above-discussed use of IDNs as a way to increase accessibility and inclusivity– while governments could lead the effort with UA-ready system procurement processes, private sector could play a role by creating incentives such as a better placement on search engine searches for websites/applications with digital inclusion aspects implemented (e.g. use of IDNs and local content).

On the wider strategy of procuring accessible ICT equipment, governments could also work closely with the private sector to fund the provision of similar technologies. Further, policies and legislation should encourage infrastructure development and commercial initiatives for increasing accessibility and inclusivity, especially in areas with geographical, demographic, and discriminatory barriers.

Capacity building to address digital divide

When addressing the digital divide issue, capacity building and digital skilling are equally important. Referring to the Indira Gandhi Smartphone Scheme in which physical resources (i.e. smartphones) were provided to women and students, more emphasis should also be placed on ensuring digital literacy and safe use (i.e. safe from cybercrimes like online sexual harassment, identify theft, and others) of the devices.

With increasing use of the Internet, applications, and digital content, it is vital to ensure media literacy among all users, especially vulnerable groups such as youths, elderly and others. In addition to basic literacy skills, investing in professional development capacity building efforts could also lead to a more diverse and robust workforce in the APAC region.

The role of youth

As current and future leaders, youth have significant capabilities and potential to shape the future of the Internet. The Internet Society Youth Policy Statement[7] has been a testament to the

[7] The Internet Society's Youth Standing Group Contribution to the United Nations Consultation on the Global Digital Compact, "Youth Perspective on the Global Digital Compact". March 2023. https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/GDC-submission_Internet-Society-Youth-Standing-Group.pdf

importance of supporting youth participation in IG, allowing youths to discuss and present their unique views on ongoing challenges and issues.

It is vital to continue to support youth participation within the IG ecosystem. In addition to funding their participation, other areas include providing support to youth initiatives, opportunities to upskill, as well as facilitating connectivity and networking among youths and with other stakeholders.

The Internet Governance Forum platform can provide support through collaboration with youth organisations and initiatives, helping to amplify the voice of youths. Such efforts can be carried out through support to national, sub-regional and regional youth IGF initiatives and offering opportunities for youths to progress within the IG ecosystem.

Protecting youths' social activities and political views on the Internet is also crucial to increasing and retaining youth participation in IG. Barriers to accessing information and expressing views online could be a cause of minimal or reducing youth participation in IG dialogues. Youth voices must be heard at local, regional, and global IG events.

A good example of "hearing youth voices" at the IGF are activities coordinated through the Youth Standing Group (which forms the IGF Working Groups Sub-Committee annually). The Youth Standing Group has launched its own consultation process to enable youth members to share their views on matters of concern. Within the APAC region, the second APAC Youth Leaders Dialogue was also held during AP yIGF 2023 with representatives around APAC participating and sharing on how to build collaborative partnerships[8]. The IGF Youth Summit at the annual IGF is also a key initiative to allow youths participating from around the world to connect. These ongoing efforts are essential to further youth involvement and participation.

[8] 2023 APAC Youth Leaders Dialogue: https://yigf.asia/page21.html

Trust

The adoption of emerging technologies can only be meaningful if communities repose their trust in the processes (and key personnel) behind the former. Online safety, digital security, free and accurate flow of information, data privacy and cybersecurity, in general, all impact the formation and breaking of trust. However, trust in global, regional and national Internet governance (IG) processes is no less critical. Same for laws and policies meant to regulate the digital ecosystem at the national level.

Trust and accountability have to be discussed together because in order to foster growth and innovation, there needs to be a certain level of trust among stakeholders. However, that trust can only be sustained if there are measures in place to ensure accountability. Once communities see how stakeholders are held accountable for their actions, trust will grow. Only when there is trust across different stakeholders (including governments, civil society, technical community and academia), can a trustworthy global digital landscape be established.

While it has been argued that current times can be characterised as post-truth, and establishing trust in such an environment can be challenging, we need to develop innovative solutions to foster trust in the Internet, including the processes and infrastructure that underpin it. For example, the idea of mathematical trust, wherein two parties interacting or transacting on the Internet can trust each other by relying on mathematical principles, can be considered by stakeholders in the APAC region and beyond as a solution. Wider adoption of blockchain technology, which has mathematical trust at its core, may be helpful in fostering trust in the Internet.

Strong encryption of personal data and end-to-end encryption of data in transit are also important measures for establishing trust. The long-term impact of ideas such as client-side scanning should be considered, and a watch should be kept on actors that are pushing to break or weaken encryption and the protection of data and communications.

Trust in Internet technologies can only be sustainable if the concerns of youths, children and marginalized communities are taken into account. The idea of consent is closely linked to trust a user poses in a platform. In order to establish an environment of trust between stakeholders (especially with end users and the private sector), ways to obtain informed and easy-to-understand consent should be devised, and the option to withdraw consent and delete user data should be provided.

Securing the cyberspace

With increasing adoption of emerging technologies, the issue of cybersecurity becomes a crucial one. Further, the COVID-19 pandemic has contributed to a dramatic rise in the use of digital technology, which has increased the attack surface for cybercriminals. While efforts are being made by individual industries, governments and civil society, it is crucial for all —

especially in APAC— to enhance collaboration in forming a trustworthy cybersecurity governance architecture.[9]

The most important and contentious geopolitical resource today is information. Data-driven innovation is transforming international relations in addition to upending economies and societies. Democracies must create new national security and economic plans that take into account the geopolitics of information if they want to compete and succeed in the twenty-first century.

Securing cyberspace in APAC and beyond will require initiating and continuing discussions on emerging technologies such as 5G, Artificial Intelligence (AI), structural architectural advances in Service Based Architecture, zero trust, deployments and secure certificate management. There is also a need to explore programs and educational efforts aimed at teaching people how to use the Internet safely, protect their data, and recognize online threats.

Gaps in the Pacific Islands

Some geographies — like the Pacific Islands[10] — are overlooked in the debates on cybersecurity. In the Pacific, the Internet brings together distant islands in national conversations. It also strengthens the Pacific voice in the face of climate change. Threats to Pacific connectivity risks diminishing and disrupting the region's voice. There has recently been a spike in cyber incidents around the Pacific islands, especially in parts of Fiji and Tonga, which has been often overlooked compared to other geographies which are well covered in the media. There is an imbalance of deployment of technology in the Pacific Islands compared to other developed regions; there is also a rise in cyber incidents in the Pacific. The gaps in technical, policy and business aspects of cybersecurity must be addressed in the Pacific Islands. Technical safeguards should be put in place to address the impact at the human level, especially financially to the civilians in the Pacific Islands.

The success of digital transformation in the Pacific and increased Internet connectivity of Pacific Islands is unfortunately accompanied with greater vulnerability of local IT systems. The recent spike in high profile, publicly reported cyber incidents from the Pacific has seen a much welcomed boost in awareness and focus on bolstering technical, organisational, and policy approaches to help increase nations' cyber resilience.

Technology is being employed as an enabler to build and strengthen services. In Tonga, the Digital Government Strategic Framework (2019-2024) sets the use of information and communication technologies for improving government decision making, business process and workflow efficiency, and improving the quality and delivery of government services while reducing the associated complexity and cost.

[9] "Stronger together: Amplifying multistakeholder voices in cyber diplomacy", https://forms.for.asia/proposal/?proposalform=NjQ1ZGRhY2UxNmJlMy8vMjMvLzEyODMvLzA=
[10] "Stories from the Pacific – the human side of cyber incidents", https://forms.for.asia/proposal/?proposalform=NjQ2MGUzNzE0YTg2Mi8vMjMvLzEzMjEvLzA=

Securing physical infrastructure, ensuring privacy in information flows, and protection of national critical data are fundamental to the Tongan government's digital strategic goals. Tonga's computer emergency response team (CERT) was established in 2016 and operates under the Ministry of Meteorology, Energy, Information, Disaster Management, Environment, Climate Change and Communications. The limited staff at CERT Tonga looks after all cybersecurity related matters for the Kingdom of Tonga. In the area of workforce development, young Tongan tertiary students are encouraged to consider an internship at the CERT if they wish to develop their cybersecurity skills. CERT Tonga also has a cybersecurity workforce development programme in partnership with the CERT New Zealand.

Developing gender-response cybersecurity policies

Women and girls are disproportionately affected by cyberbullying, online harassment, and stalking. They are also more likely to be victims of identity theft and online fraud. Additionally, women and girls are often underrepresented in the cybersecurity field. This means that they are less likely to have the skills and knowledge to protect themselves from cyberattacks. adopting gender-responsive cybersecurity policies[11] that takes into account the unique risks and challenges faced by women and girls in the digital world.

A gender-responsive cybersecurity policy can help to address these challenges by raising awareness of the unique risks and challenges faced by women and girls in the digital world, and providing resources and support to help women and girls protect themselves from cyberattacks, as well as supporting the participation of women and girls in the cybersecurity field.

Some recommendations for developing a gender-responsive cybersecurity policy that can be implemented within APAC economies:

- Conduct a gender assessment of cybersecurity risks and challenges. This will help to identify the specific needs of women and girls in the community.
- Develop policies and procedures that are gender-sensitive. This includes considering the needs of women and girls when developing technical solutions, such as authentication and authorization systems.
- Provide training and awareness-raising to all employees on gender-responsive cybersecurity. This training should cover topics such as cyberbullying, online harassment, and online fraud.
- Support the participation of women and girls in the cybersecurity field. This can be done by providing scholarships, mentorship programs, and other forms of support.

The best approach will vary depending on the specific context of each economy. The recommendations above provide a starting point for developing a policy that will help to protect all people from cyberattacks, regardless of gender.

[11] "Framework for Developing Gender-responsive Cybersecurity Policy", https://forms.for.asia/proposal/?proposalform=NjQ2MGYyMTFlYWI1ZS8vMjMvLzEzMjIvLzA=

It is also important to ensure that gender-responsive cybersecurity policies are developed and implemented in a participatory and inclusive manner. This means involving women and girls in the policy development process and ensuring that their voices are heard. It also means considering the needs of different groups of women and girls, such as those from marginalized communities.

Balancing data privacy, safety and security concerns

The APAC region is increasingly becoming a target for cyberattacks, with governments and law enforcement agencies (LEAs) increasingly using security measures to protect users from harm. However, certain actions taken to address online safety issues can have negative consequences, including but not limited to the following: [12]

- Undermining user privacy: When security is broken, it will be easier for malicious actors to intercept and steal sensitive data. This can put users' privacy at risk.
- Eroding trust in online platforms: When users know that their security is not guaranteed, they are less likely to trust online platforms. This can make it difficult for businesses to operate and for individuals to access essential services.
- Enabling government surveillance: When governments break security for online safety, it gives them more tools to monitor and control their citizens. This can be used to suppress dissent and silence marginalized voices.

In recent years, there has been a growing trend of governments and LEAs in the APAC region breaking security for purposes of enhancing online safety. This includes measures such as mandating backdoor encryption, requiring social media platforms to remove harmful content, and conducting surveillance of online communications.

For example, in China, the government requires all social media platforms to operate under a real-name registration system. This allows the government to track and monitor users' online activities. The Chinese government also has a strict censorship regime that requires social media platforms to remove content that is deemed to be subversive or harmful to national security. In India, the government has passed a number of laws that give it broad powers to surveil online communications (e.g. the Information Technology Act allows the government to intercept and monitor communications without a warrant). Other countries in the APAC region, such as Vietnam, Indonesia, and Thailand, have also passed laws that restrict online freedom and give the governments more power to surveil its citizens.

It is important to find a balance between protecting users from harm and promoting trust in the digital economy. This can be done by developing transparent and accountable content moderation policies, by ensuring that security measures are not used to undermine user privacy, and by promoting the use of open source and interoperable technologies.

[12] “Breaking security for ‘online safety’: What’s at stake for Asia-Pacific”, https://forms.for.asia/proposal/?proposalform=NjQ1MzkzNmMyZGJjOS8vMjMvLzEyNDcvLzA=

The following are some recommendations for addressing the challenges of online safety and security in the APAC region:

- Governments and law enforcement agencies should avoid breaking security for the purposes of online safety. Instead, they should focus on measures that protect user privacy and security, such as investing in cybersecurity education and promoting the use of strong encryption.
- Social media platforms and other online platforms should develop transparent and accountable content moderation policies. These policies should be developed in consultation with stakeholders, including civil society organizations and representatives of marginalized groups.
- Governments should promote the use of open source and interoperable technologies. This will make it more difficult for governments to censor the Internet and will give users more control over their data.

Content moderation policies

Content moderation policies are used by social media platforms and other online platforms to remove harmful content, such as hate speech, misinformation, and disinformation. These policies can play an important role in protecting users and promoting democracy online.

However, content moderation policies can also be used to stifle dissent and silence marginalized voices.[13] For example, governments can pressure social media platforms to remove content that is critical of the government or that challenges the status quo. Additionally, social media platforms can use their content moderation policies to promote their own business interests, even if this means suppressing certain types of content.

There are a number of ways that content moderation policies can be used to advance technology for democracy. For example, these policies can be used to:

- Protect users from harmful content: Content moderation policies can be used to remove harmful content, such as hate speech, misinformation, and disinformation. This can help to create a safer and more welcoming online environment for all users.
- Promote freedom of expression: Content moderation policies can be used to protect users' right to freedom of expression. This includes protecting the right to express dissent and to challenge the status quo.
- Support marginalised groups: Content moderation policies can be used to support marginalised groups by protecting them from online bullying, harassment, and discrimination.
- Increase transparency and accountability: Content moderation policies can be used to increase transparency and accountability in the tech sector. This can help to ensure that content moderation decisions are made in a fair and impartial manner.

[13] "Content moderation policy advancing technology for democracy", https://forms.for.asia/proposal/?proposalform=NjQ2MTc0YzExYzY1MC8vMjMvLzEzNTQvLzA=

There are a number of challenges and opportunities associated with using content moderation policies to advance technology for democracy. It can be difficult to define what constitutes harmful content. This is especially true in the context of social media, where there is a wide range of user-generated content.

Balancing freedom of expression and protection from harm, content moderation policies need to strike a balance between protecting users from harm and respecting their right to freedom of expression. This can be a difficult task, especially in cases where the two values conflict. Content moderation policies need to be implemented in a way that prevents bias and discrimination. This can be a challenge, especially given the complexity of AI algorithms that are often used to moderate content.

Following are some ways through which content moderation can be improved:

- Using technology to improve content moderation: Technology can be used to improve the accuracy and efficiency of content moderation. For example, AI algorithms can be used to identify harmful content at scale.
- Promoting transparency and accountability: Content moderation platforms can increase transparency and accountability by providing users with more information about how content moderation decisions are made.
- Engaging with stakeholders: Content moderation platforms can engage with stakeholders, such as civil society organizations and representatives of marginalized groups, to develop and implement content moderation policies that are fair and inclusive.
- Guidelines for trusted notifiers: Civil society, technology community, law enforcement agencies and governments need to work together on developing a guideline at the APAC level for trusted notifiers.

Creating a safe digital space for future generations

Children are growing up in a world where technology is increasingly pervasive, and their data is being collected and used in a variety of ways. This presents both opportunities and risks. On the one hand, children can benefit from access to information and educational resources, and from the ability to connect with friends and family members from all over the world. On the other hand, children are vulnerable to online predators, cyberbullying, and the misuse of their data.[14]

It is essential that we co-create a digital future for children that protects their rights and well-being, while also allowing them to benefit from the opportunities that technology has to offer. This requires an intergenerational, multistakeholder dialogue. Children themselves must have a voice in shaping the digital world that they will inherit. Governments, businesses, civil society organizations, and parents also have a role to play.

[14] "Co-creating Digital Future for Children: An Intergenerational, Multistakeholder Dialogue on Children's Data Protection", https://forms.for.asia/proposal/?proposalform=NjQ1ZjliZjQ2ZTIxNy8vMjMvLzEyOTQvLzA=

There are a number of key issues that need to be considered in co-creating a digital future for children. These include:

- Data protection: Children's data is particularly sensitive, and it is important to protect it from unauthorized access and misuse. This can be done through a combination of legal and technical measures.
- Online safety: Children need to be protected from online predators, cyberbullying, and other forms of harm. This can be done through education, awareness-raising, and technical measures such as parental controls.
- Digital literacy: Children need to be equipped with the skills, knowledge and agency they need to navigate the digital world safely and responsibly. This includes developing their critical thinking skills and their ability to identify and avoid misinformation.

The following are some recommendations on different stakeholders' roles for co-creating a digital future for children:

- Governments should develop and implement comprehensive laws and policies to protect children's data and online safety. These laws and policies should be developed in consultation with children themselves, as well as with other stakeholders such as businesses, civil society organizations, and parents.
- Businesses should adopt responsible data collection and processing practices. This includes obtaining consent from parents or guardians before collecting or using children's data, and using the data only for the purposes for which it was collected.
- Civil society organizations should play a role in educating children and parents about digital literacy and online safety. They can also work to develop and promote child-friendly technologies.
- Parents and children should learn more about online safety and help develop healthy digital habits. They should also be aware of the risks and benefits of online technology, and take steps to protect their personal data.

Impacts of data protection laws

Data protection laws in the APAC region have become a significant topic of discussion in various economies, including Indonesia, India, and the Philippines. These laws aim to protect personal data processing and grant data subjects more control over their data.

However, despite their well-intentioned goals, some provisions within these data protection laws pose threats to civic freedoms, including freedom of expression and the press.[15] Such laws can inadvertently shrink the operational space for civil society organizations.

[15] "To protect or harm?: what the tensions between privacy and civic freedoms in personal data protection laws mean for civil society", https://forms.for.asia/proposal/?proposalform=NjQ2MTliMGFhYmZiZS8vMjMvLzEzNjIvLzA=

The risks associated with data protection laws include:

- Disproportionate compliance costs are imposed on data controllers across various sectors.
- Potentially leading to financial and reputational risks.
- Eroding trust from donors and supporters.
- Misuse of these laws to stifle criticism and dissent, as seen in cases like Hungary and Greece, where the European Union General Data Protection Regulation (EU GDPR) was used against media organisations.

There is a need to identify potential solutions to address these challenges and maintain civil society resilience in the face of evolving data protection laws.

Indonesia

Indonesia's Personal Data Protection Law has raised concerns among Civil Society Organisations (CSOs) due to its lack of technical safeguards, designated data protection officers, and potential backlash. The law focuses on personal data protection, excluding non-personal data, and requires consent for data processing. However, some exemptions allow data processing without explicit consent, raising concerns about government powers. The Act establishes a data protection board, but its independence and composition remain concerning.

India

Similarly, the Aadhaar system collects extensive personal data in India, including fingerprints and retina scans. The Right to Information Act in India could limit access to information, and excessive delegation of authority to regulations raises questions. Penalties for data breaches differ for data principals and fiduciaries, with potential implications for CSOs. Additional obligations for significant data fiduciaries may increase compliance costs and impact CSO operations.

Philippines

In the Philippines, data privacy laws aim to ensure the lawful handling of personal data while safeguarding human rights and privacy. However, they can be subject to abuse, misinterpretations, and government actions that can limit access to information. CSOs need help complying with data privacy laws, including financial constraints and a lack of trained personnel. To enhance resilience, CSOs can upskill, participate in policy-making processes, and collaborate with other CSOs. Transnational collaboration is essential in advocating for robust data protection while safeguarding civic freedoms.

Compliance with laws

Strengthening the support network for CSOs, including legal experts, public advocates, and digital security experts, is crucial for compliance with data protection laws and data privacy advocacy. Some examples of ongoing efforts to build capacity and address specific challenges are:

- Identifying and targeting groups that have yet to receive training on digital security and data privacy to ensure that capacity-building efforts are practical.
- Developing privacy policies within organizations to enhance compliance with data protection laws.
- Supporting litigation efforts related to digital rights and data protection.

Connecting and forming alliances among data privacy activists and advocates globally and regionally, particularly in APAC, is essential to work towards more rights-respecting and proportionate data protection laws collectively.

A case study on Indonesia

Data collection processes in Indonesia, particularly for programs like societal protection, have become extensive and increasingly automated in recent years. While the concepts of data application and data justice are crucial, they often lack real-world examples. The Village Information System (VIS) in Indonesia plays a vital role in this context, and the principles of data justice can be used to analyse the implementation of data collection programs.[16]

Indonesia's vast population and social protection programs necessitate substantial data collection efforts, but the impact of data analysis still requires determination. Data sovereignty is a significant concern, especially at the local and village levels. The VIS, mandated by law, supports social protection programs by collecting and analyzing data. Various actors are involved in data collection programs, and initiatives like public data trusts aim to coordinate them for better governance. Challenges include consent, data storage, compensation, and public data safety.

Indonesia's pursuit of sustainable development relies heavily on evidence-based policy-making, particularly at the national and local levels. However, a significant challenge lies in the fragmented nature of official data, with ministries and agencies needing to share data with regional governments and villages more effectively. To address this, the Indonesian government introduced the Electronic Based Government System and One Data Indonesia policies to enhance data integrity through integrated governance. Nevertheless, there's room for improvement in their digital transformation strategy, especially concerning data justice considerations.

Promoting effective collaboration between government agencies and civil society is a multifaceted challenge. While some governments have established petition platforms that empower individuals and groups to voice their concerns and trigger responses from regulatory authorities, fostering improvements in public services and policies, such mechanisms are not

[16] "The Fulfillment of the Data Justice Framework through the Data Governance Model in Implementing the Village Information System; Indonesia Case Study", https://forms.for.asia/proposal/?proposalform=NjQ2MTY2NmFkYjgzZi8vMjMvLzEzNDYvLzA=

universally embraced, especially in culturally diverse contexts and when dealing with complex issues like data.

The possible privacy, technology-related, and discrimination challenges associated with implementing the VIS represent the most basic form of data management within the bureaucratic framework. To address these issues, the Public Data Trusts (PDTs) model for VIS can be adopted and cooperative efforts between government agencies and civil society should be promoted. Ensuring the protection of data sovereignty for village communities is of the utmost importance throughout this endeavor.

In Indonesia, for instance, the government is crafting ethical guidelines for AI and regulations for data scraping, seeking input from civil society to ensure a well-rounded perspective in the policy-making process. This consultation serves as a vital avenue for civil society to share their views and insights.

Contours of AI regulation

There is an urgent need to focus on AI ethics and regulation as some governments (especially in South and South East Asia) and private sectors employ AI tools for undermining the rights of peoples of the region. Academia and civil society along with other stakeholders need to work together in finding, highlighting and addressing the potential dangers of AI.

The APAC region has vast cultural, social, and economic diversity. Even the forms of governments vary across economies. It is important to factor in this diversity when studying the impact of AI within the region.

Current legislation relating to AI focuses on varying aspects from national security to personal privacy protection. Stakeholders should attempt to develop a base framework that could be applicable across different jurisdictions, similar to a set of universal standard good practice. The framework should outline approaches for responsible use of technologies, and encompass fair and transparent factors. Such a framework should complement existing regulations (e.g. the EU GDPR) and standards (e.g. UN SDG principles).

In addition, safeguards need to be placed for preventing the use of AI for spreading disinformation and producing echo-chambers, especially during elections.

AI and the job market

While there are genuine apprehensions about the negative fallout of the AI applications, especially on the job market, AI can also be used for positive purposes. Lessons can be drawn from the Industrial Revolution which also initially sparked worries about the impact of machines on labour. But human societies found ways to adapt, lift people out of poverty, and increase productivity.

Large language models (LLMs) are being developed at a rapid pace, but these are mostly concentrated in the United States. There is a need to develop LLMs in the APAC region preferably with an open-source architecture. People of the APAC region not just need to be consumers and data providers for LLMs made elsewhere, but should also be developers of LLMs.[17]

Economies like Japan, South Korea, India, and China have taken steps towards AI governance. It is noted that ASEAN is developing a guardrail governance code document for guiding AI, with a planned 2024 release[18]. Other economies in the APAC region need to expeditiously create appropriate frameworks to govern and regulate AI.

While investing resources in AI regulation is important, it is also equally important to invest in societies — because people are the ultimate users of AI and it is on their usage patterns that the potential of AI to create or destruct depends.[19]

Mitigating biases in AI models

Biases in AI models is a hot topic of discussion in the region. Bias in AI tools leads to discrimination of marginalised communities. There is an urgent need to design AI tools that limit bias, and enable — rather than discriminate — marginalised communities across the region.

Fostering accountability and transparency in all stakeholders

Inclusive dialogue as a foundation for shaping governance builds trust, especially when diverse cultures and views need to be acknowledged. Future development of the current multistakeholder model needs to address how certain stakeholders do not feel included.

As efforts on Internet regulation differ by region, economy, or jurisdiction, a comprehensive publicly available repository of global attempts—such as the Tech Policy Atlas[20]—serves to build trust and advance the development of Internet governance.[21] Barriers in accessing existing databases inhibit evidence-based independent research and the development of actionable suggestions to governments/industries—and ultimately cause undermining of trust.

This echoes the driving force behind APrIGF's own Synthesis Document, which is also a collaborative and collective effort, which later becomes publicly available output[22].

---

[17] "AI in Asia-Pacific: Charting a Path for Responsible Innovation". https://forms.for.asia/proposal/?proposalform=NjQ1N2JkN2I4YmY3Yi8vMjMvLzEyNTQvLzA=
[18] Potkin, Fanny and Wongcha-um, Panu. "Exclusive: Southeast Asia to set 'guardrails' on AI with new governance code". *Reuters*. 16 July 2023. https://www.reuters.com/technology/southeast-asia-set-guardrails-ai-with-new-governance-code-sources-2023-06-16/
[19] Ibid.
[20] Tech Policy Atlas: https://techpolicydesign.au/tech-policy-atlas
[21] "Tech Policy Atlas: your one stop shop for Internet law, regulation and strategy", https://forms.for.asia/proposal/?proposalform=NjQ2MGQyZGI2ZDJiMS8vMjMvLzEzMTgvLzA=
[22] "Evolving Internet Governance For The Next Phase Of The Internet", https://forms.for.asia/proposal/?proposalform=NjQ2MGQyZGI2ZDJiMS8vMjMvLzEzMTgvLzA=
[13] Ibid.

Sustainability

Recent Internet governance discussions have focused on ensuring the sustainability of the Internet and other digital technologies, by assessing their social, economic and environmental impacts. The idea of sustainability permeates the international, regional, national and local levels alike. The Dynamic Coalition on Environment[23], initiated by the IGF is a reflection of the importance and relevance of the topic of sustainability in present times.

Emerging technologies can cause further disruptions to this ecosystem, not only to the socio-economic and political fabric of the community but also to our physical environment. They could have considerable impact on the ongoing climate crisis, and affect local communities that are at the forefront of the fight for climate justice. Further, these new technologies have the potential to disrupt the regional economy, particularly the labor economy in many known and unforeseen ways.

A multifaceted strategy is required if these technologies are to be sustained over the long run. Its core criterion is universal accessibility to dependable and resilient connection, even during crises, wars, or natural catastrophes. This fundamental element serves as the framework for the sustainable development of the Internet and emerging technologies, and ensures that they contribute to a more equitable future for all.

We are situated at the intersection of societal well-being, ecological harmony, and technological growth. The solution calls for a multidisciplinary symphony in which ethical questions, social inclusion, and environmental responsibility dance with technical progress. By balancing these factors, we must direct the process of developing technologies to live up to their potential as builders of a just and sustainable digital future.

There is also a need to consider the sustainability of the multistakeholder model. Questions arise for how to re-gather support for this model globally, as well as how we can improve the approach and practice nationally, regionally, and globally.

Internet for a sustainable environment

The idea of sustainability for the environment encompasses various aspects of ICT and allied subjects. These include green technologies, energy efficiency, renewable energy, carbon emissions reduction, environmental impact of new technologies, data-driven impact assessment, environmental legislation, environmentally conscious production processes, sustainable lifecycle management of devices, e-waste reduction, circular economy, and circular design principles.

[23] Dynamic Coalition on Environment: https://www.intgovforum.org/en/content/dynamic-coalition-on-environment-dce

Managing e-waste

On the use and disposal of smartphones, engaging the youth community raises awareness of the resources that are used for making smartphones[24]. Today, 45% of the world's Internet users are below the age of 25. Young people are increasingly living their lives in the digital domain, as education, entertainment, social life and commerce become online activities, a trend exacerbated by the COVID-19 pandemic.

While invented only thirty years ago, smartphones today impact all aspects of our lives. However, school curricula today do not address how smartphones contribute to global e-waste majorly, and consist of elements which may have harmful impacts on communities and ecologies they are mined in.

Moreover, elements in the smartphone have a low recycling rate, making sustainable sourcing and recycling a challenge. This added to the problem of planned and perceived obsolescence makes phone replacement rates a wasteful exercise which is not just costly for consumers, but also deeply damaging to the planet.

Educating youths on the full life cycle and materials used for smartphones increases awareness and encourages more conscious behaviour when "consuming" the technology. Various stakeholders (e.g. researchers, educators, policymakers, parents, civil society) play a role in reaching out to youth in engaging ways to understand technology and sustainability in a personal way.

Digital environmental sustainability through circular economy and sustainable design solutions

Solutions such as open-source designs, industry incentives for circular practices, lower operational costs, responsible consumption, and leveraging the big tech, could be potential solutions for environmental sustainability[25]. With the increasing demand for digital devices, the impact is becoming increasingly pronounced in the Global South and in South Asian countries like India.

A key issue is the use-and-throw culture without considering the environmental impact of their actions. Secondly, with increasing digital linear consumption, the extraction of minerals and other resources is putting significant pressure on the planet's resources, including rare earth metals and other critical minerals. Furthermore, digital devices are energy-intensive to produce and significantly contribute to greenhouse gas emissions.

Thus, there is growing need and priority to transition to a more circular economy model for digital devices that involves reducing waste, reusing and repairing devices, and recycling materials to create new products. This involves implementing use-repair and reuse culture, and developing and promoting desired social and behavioral change. Early experiences from

[24] "Mines, Maps and Minerals: Trace the complex material flows of your smartphone to make more sustainable choices", https://forms.for.asia/proposal/?proposalform=NjQ2MTVlZDI3NGRlZC8vMjMvLzEzNDQvLzA=
[25] "Digital Environmental Sustainability through Circular Economy and Sustainable Design Solutions", https://forms.for.asia/proposal/?proposalform=NjQ1ZmUyZTFlNGNjMi8vMjMvLzEyOTUvLzA=

economies like India and evolving models like ‘Digital Green Prakriya’[26] could be adopted across the region.

This also calls for sustainable human rights-centered design solutions which involves designing products with human rights in mind, such as fair labor practices, and using materials that are environmentally sustainable, and designing products that are easier to repair and reuse.

By promoting a circular economy in digital devices, positive impact downstream and upstream can be achieved. A natural shift to a circular model calls for willing collaboration and innovation from manufacturers, consumers, policymakers, and other stakeholders.

Sustaining efforts to overcome digital divides through community initiatives and practices

Community driven initiatives to overcome the digital divide are essential. Local projects play an essential role in providing Internet access to underserved areas which are often neglected by larger Internet service providers. However the focus should not only be on connectivity provision but also on ensuring that the Internet translates into practical benefits for improving their businesses, skills and overall quality of life.

Sustainability and reliability emerged as critical concerns. It is vital to find affordable and environmentally friendly ways to provide easy Internet access. This involves using innovative technologies to reduce cost and the impact on the environment. In terms of overcoming the challenge of high costs in remote areas, collaboration with larger industries to explore cost effective solutions could be potential strategies.

To strengthen such initiatives, community networks can be integrated with local businesses and development efforts. Community networks can serve as platforms for businesses to reach new customers and enhance their operations, particularly in rural regions where such opportunities are limited.

Ongoing learning, collaboration, and digital skill development are essential in narrowing the digital divide and empowering communities to harness the Internet for their benefit. For instance, libraries have a unique reach and in the case of school libraries, trained librarians have been empowering students with media and information literacy skills for a long time. If the Internet we want is a healthier information ecosystem then we need to call for Information Integrity on Digital Platforms[27].

As such, community-led initiatives play a vital role in bringing positive impact on Internet access to underserved populations.

---

[26] Digital Green Prakriya (Processing). "Fostering Digital Environmental Justice through Community Repair and Reuse Network in India: A Pilot Report 2022-2023" https://www.defindia.org/wp-content/uploads/2023/05/DGP-Pilot-Report.pdf

[27] United Nations. "Our Common Agenda Policy Brief 8 Information Integrity on Digital Platforms". June 2023. https://www.un.org/sites/un2.un.org/files/our-common-agenda-policy-brief-information-integrity-en.pdf

Sustainability of the Internet: Avoiding Internet Fragmentation

There have been concerns raised regarding the sustainability of a global and interoperable Internet. Some key factors causing a ‘splinternet’/Internet fragmentation are the lack of interoperability across devices with new technologies, data localization, and geopolitical tensions. As the risk of a splinternet increases, we need to work together towards building a sustainable Internet for all.

Fragmentation, and the future of the Internet

Internet Fragmentation is a term that requires clear definition and understanding. Further discussions are required to review its impacts on technical dimensions as well as on society and jurisdictions. Internet fragmentation can be perceived as both desirable and undesirable depending on the context and needs.

The main criteria for evaluating such decisions are intention (the purpose behind fragmentation), impact (who is affected and how), and the societal needs of the communities involved. The roles of algorithms and data collection in exacerbating fragmentation also need to be considered.

Algorithm-driven content filtering and recommendation systems can significantly impact the information people are exposed to, potentially reinforcing biases and limiting access to diverse perspectives. Encouraging the use of decentralized technologies and fostering a mindset of active contribution rather than passive consumption are potential strategies to counteract algorithm-driven fragmentation.

There are key concerns on the potential for overreach in regulating the Internet. While some fragmentation may be justified in addressing issues like cybercrimes, overzealous measures will pose detrimental effects on communication, trade, and development. There is a need to uphold the concept of "One World, One Internet" while acknowledging the challenges posed by jurisdictional differences.

Ongoing dialogue should be held for awareness-building, and on understanding technological advancements to comprehensively address Internet fragmentation. Multistakeholder engagement is key to addressing Internet fragmentation challenges. Collaborative discussions involving a diverse group of stakeholders, including technical experts, policymakers, civil society, and the private sector are essential in making informed decisions that balance the interests of different communities.

The topic of Internet fragmentation is multifaceted, and it is important to find a balance between safeguarding societal interests, while maintaining a universally interconnected and open Internet. Achieving this balance will require continued collaboration among stakeholders and proactive efforts to ensure that the Internet remains a tool for empowerment, education, and global communication.

Internet of Things– Impact on sustainability

The Internet of Things (IoT) has become an integral part of our everyday lives. Used at industrial and work sites, city infrastructure, and homes, there are debates on the impact on sustainability from the extensive use of these IoT devices and services.

Discussions emerged[28], and the IoT Global Good Practice Paper was presented at IGF 2018. Since then, several changes have occurred to address challenges from IoT. Nonetheless, discussions will be elevated, with the target to provide input to the High-Level Expert group from the Dynamic Coalition on IoT (DC-IoT)[29], together with the DC on Core Internet Values (DC-CIV)[30]. The input will eventually also be shared at the World Summit on Global Digital Compact in September 2024.

Also, further discussions are needed to further develop the concept of what it means to have "meaningful transparency" to all stakeholders, and "real accountability" to stakeholders that can reasonably be expected to bear responsibilities from the impacts of IoT. Focus areas can include the following:

- Introducing global good practice in IoT;
- Focusing on the need for labeling (and thus certification) to help consumers to be able to take their responsibility;
- Clarifying why approaching it as "Internet of Functions" can help.

On "Internet of Functions", IoT must include a base level of security elements. The "Internet of Functions" define functions that determine the needed level of cybersecurity. When discussing at the global level, it is key to adopt the approach of "zero trust".

The concept of "zero trust" covers the following elements:

- Maintaining independence of apps from hardware (Internet of Functions);
- Developing a data centric approach with transparency for 'who' and 'how' to use the data;
- Integrating interoperability at the technical level with legacy systems. Security by design, zero trust, and identification as the order of self/group/public help for cybersecurity is a mandatory requirement.

Currently when purchasing an IoT device, there is general lack of information on whether and what data would be transmitted through the device, as well as the level of security and options to secure the devices. There are no legal or self-regulatory actions currently in place, but initiatives are underway.

[28] "Progressing Core Internet Values and Global Good Practice for the Internet of Things: impact on sustainability", https://forms.for.asia/proposal/?proposalform=NjQ1ZTEyOWRkZGUwMy8vMjMvLzEyODUvLzA=
[29] Dynamic Coalition on IoT: https://www.intgovforum.org/en/content/dynamic-coalition-on-the-Internet-of-things-dc-iot
[30] Dynamic Coalition on Core Internet Values: https://www.intgovforum.org/en/content/dynamic-coalition-on-core-Internet-values-dc-civ

For instance, the Five Eyes (FVEY) nations — United States (US), United Kingdom, Canada, Australia, and New Zealand — issued a Statement of Intent in 2019 regarding the security of IoT. The statement recognised that this issue is global. In Europe, there is a Cyber Resilience Act that also covers some aspects of IoT. Also in the US, the Biden administration recently introduced a new initiative to empower consumers to make decisions about the security of IoT devices. The US Cyber Trust Mark is a voluntary public-private partnership enabling manufacturers to self-certify that their products meet essential cybersecurity standards.

Conclusion

To safeguard the digital future, ongoing multistakeholder discussions and collaboration are required. While some existing barriers remain (e.g. time zone differences, financial/resource constraints or limitations to participate), we need to work collectively to create platforms for these discussions, and encourage diverse participation from different stakeholders across the region.

This includes meaningful engagement across various stakeholders such as governments, businesses, civil society, academia, and others. Regional collaboration and partnerships are also vital towards building a shared vision for a trusted, inclusive, and sustainable Internet.

Key input from regional discussions (e.g. this Synthesis Document) should also be brought forward to global platforms such as the global IGF, Global Digital Compact, and WSIS+20 processes, to ensure voices from the APAC region are heard and considered.

Appendix I

Full affiliation list for 2023 Drafting Committee:

Name	Affiliation	Stakeholder group	Track
Yien Chyn Tan (Co-chair)	ICANN	Technical Community	Access & Inclusion track lead
Amrita Choudhury	CCAOI	Civil Society	Access & Inclusion
Waqas Hassan	Assistant Director (International Liaison Training), Pakistan Telecommunication Authority	Government	Access & Inclusion
Charlotte Fang Hendro	University of New South Wales	Civil Society	Access & Inclusion
Mohammad Ali Jauhar	ISOC Youth Standing Group	Technical Community	Access & Inclusion
Winston Roberts	IFLA (International Federation of Library Associations)	Civil Society	Access & Inclusion
Shradha Pandey	Youth Standing Group, Board Member, ISOC	Civil Society	Sustainability track lead
Uzair Farooqi	Pakistan Mobile Communication Limited (Jazz, PMCL)	Private sector	Sustainability
Brian Mangi	ITSUP Ltd	Private sector	Sustainability
Lokendra Sharma (Co-Chair)	National Institute of Advanced Studies, Bengaluru	Academia	Trust track lead
Dr. N. Sudha Bhuvaneswari	Dr. G. R. Damodaran College of Science	Academia	Trust
Minkyoung Cho	Deloitte Tohmatsu Cyber	Private sector	Trust
Cherie Lagakali	GFCE Senior Advisor	Technical Community	Trust
Dr. Saima Nisar	Universiti Utara Malaysia	Academia	Trust
Agita Pasaribu	Bullyid App (NMA Foundation)	Civil Society	Trust
Abdullah Qamar	Virtual University of Pakistan	Academia	Trust
Stella Anne Teoh Ming Hui	Kyushu University, NetMission.Asia	Civil Society	Trust

Appendix II

2023 APrIGF workshop sessions:

	Workshop
1	AI in Asia-Pacific: Charting a Path for Responsible Innovation
2	Investing in professional development for a diverse workforce in APAC: challenges and opportunities
3	Sustainability of Complementary Connectivity Initiatives
4	Policy development on generative AI based on Biometrics & Weaponizing Information Bubbles
5	Stronger together: Amplifying multistakeholder voices in cyber diplomacy
6	Breaking security for 'online safety': What's at stake for Asia-Pacific
7	Content moderation policy advancing technology for democracy
8	Disability and Digital Self-Determination: What's the Missing Link?
9	Co-creating Digital Future for Children: An Intergenerational, Multistakeholder Dialogue on Children's Data Protection
10	AI & Gender in Asia Pacific
11	The role for government purchasing of accessible Information and Communications Technology (ICT)
12	To protect or harm?: what the tensions between privacy and civic freedoms in personal data protection laws mean for civil society
13	Progressing Core Internet Values and Global Good Practice for the Internet of Things: impact on sustainability
14	Stories from the Pacific – the human side of cyber incidents
15	Tech Policy Atlas: your one stop shop for internet law, regulation and strategy
16	The Fulfilment of the Data Justice Framework through the Data Governance Model in Implementing the Village Information System; Indonesia Case Study.
17	Ambivalence in Fulfillment of Internet Access Rights in West Papua? Civil Society Experience
18	Youth Engagement in the Asia Pacific: What does the future hold for young people? – A showcase from Youth Standing Group
19	Online Safety Self regulatory Codes of Practice as a means to tackle digital harms – the New Zealand experience
20	Be Safe Project
21	A Framework for Developing Gender-responsive Cybersecurity Policy
22	Unpacking stakeholder engagement with the private sector

23	Mines, Maps and Minerals: Trace the complex material flows of your smartphone to make more sustainable choices
24	Bridging the Communications Divide
25	Connecting Communities: Community Radio for Connectivity, Inclusion, Digital Rights, and Freedom of Expression
26	Is fragmentation the future of the Internet and How Can We Resist?
27	Exploring Youth Perspectives in Social Media Content Creation
28	Internationalised Domain Names: Implementation around APAC – Lessons, Challenges & Opportunities
29	Evolving Internet governance for the next phase of the Internet
30	Digital Environmental Sustainability through Circular Economy and Sustainable Design Solutions
31	What are the Challenges, Progress and Social Prosperity for Digital Economy in Asia?
32	G20 in India and digital inclusion: The impact of shutdowns
33	Impacts of national digital transformation on small island developing states