Asia Pacific Regional Internet Governance Forum
2019 Synthesis Document

Enabling a Safe, Secure and Universal Internet for All in Asia Pacific

I. Human Rights Online

Human rights are integral to human autonomy and social justice. The Internet and other digital technologies have greatly changed the way in which we experience human rights – they not only allow us to exercise our rights online but also enable the realisation of our rights offline. It is important that human rights are respected and applied universally to the physical and the Internet space in the areas of –access and development, freedom of expression, right to assembly and privacy as well as on the right to education, health, culture and to a broad range of other rights. With the constant evolution of technology and Internet, human rights online should be ever-evolving to reflect progress in our society.

A repeated theme during the various workshops and discussions at the APrIGF this year was the cross-cutting nature of human rights on issues related to access, cybersecurity, digital economy, among others[1]. It was discussed that a rights-based approach must be implemented at every level. Internet infrastructure, both hardware and software, must be rights-respecting by design. Regulations, norms and standards for the functioning of the Internet must reinforce human rights. Companies should use human rights law as the authoritative global standard for ensuring freedom of expression and other rights on their platforms.

With issues such as online censorship, Internet shutdowns, gender-based violence and inequality, hate speech, privacy invasion increasing in countries across the Asia Pacific region, it is important to advocate for a people-centered, rights-respecting Internet.

ICT regulations, laws and norms

Advancement to digital technologies is taking place at a rapid pace, and many governments are struggling to catch up. They are reacting to potential threats through legislations on cybercrime, cybersecurity, data protection, use of social media and misinformation. While some of these regulations are much needed and long overdue, many of these laws are in fact vaguely written with scope for misuse, give sweeping powers to governments to surveil and persecute citizens in the guise of national interest, and are increasingly used to stifle online expression, and censor and criminalise speech, resulting in shrinking online spaces and reduced participation in democratic processes.

An important discussion at the APrIGF was that laws on ICTs are often designed to censor content (for example, laws around misinformation and “fake news”) and increase government

[1] WS23. Big tech everywhere: Is this the future of the Internet? https://apps.2019.rigf.asia/submission/proposaldetail?id=311

surveillance online (for example, laws around cybersecurity). Other laws, such as those related to data protection, may not place adequate restrictions on states or the private sector, leading to human rights violations. Governments are also increasingly using laws related to sedition, terrorism and blasphemy to crackdown on journalists, bloggers and others expressing dissent, chilling free speech and access to information.

Many of these laws often have a negative impact on human rights including freedom of expression, assembly and association, information and privacy among others. It is critical to analyse how these laws relating to ICTs are intended, interpreted and implemented and to understand the extent to which governments in the Asia Pacific region are preserving the security of individuals, and promoting and protecting human rights online and balancing national security within their legal framework.

A multistakeholder approach should be complemented to include multi-sectoral and multi-disciplinary stakeholders to ensure ICT legislations address the needs of and serve the public, thereby advancing and enhancing the multistakeholder framework to the betterment of Internet governance in the region.

Cross-border collaborations such as the adoption of the ASEAN Framework on Personal Data Protection and ASEAN Framework on Digital Data Governance, and the Asia-Pacific Economic Cooperation APEC Cross-Border Privacy Rules CBPR serves as examples for the advancement of our regional ecosystems in Internet governance.

Network Shutdowns

Internet connectivity is essential to the exercise of human rights, especially in times of conflict. The United Nations Human Rights Council has passed a resolution stating that any measures to intentionally prevent or disrupt access to or dissemination of information online is a violation of international human rights law. Yet, governments in the Asia Pacific region lead the world in the number of instances of network shutdowns. Governments resort to complete or partial blocking of social media or the Internet for a number of reasons, including to curb the spread of misinformation, threats and violent content, and even more so during times of social unrest or protest. Network shutdowns have a series of negative impacts on human rights including the right to access, information, education, health, expression and assembly and association. Network shutdowns are often disproportionate (such as blocking an entire website for a specific piece of content) and never adequately justified[2]. Further, they are not an efficient or effective solution to tackle complex situations.

There is a need for stronger collaboration between civil society and the private sector to tackle Internet shutdowns[3], particularly in challenging the legality of government orders, and more transparency from telecom companies and Internet service providers, who are responsible for

[2] WS.28 Honey, I shut the internet! Dealing with internet shutdowns in Asia Pacific: https://apps.2019.rigf.asia/submission/proposaldetail?id=318

[3] Ibid

implementing the shutdowns on behalf of the government, by publishing information on number of requests they receive and the reasons for such requests from states.

Digital Identity

Digital identity programmes are gaining popularity among many governments in Asia, with countries like India, Pakistan, Japan and Thailand having already implemented such programmes and others like Nepal and the Philippines soon following suit. Many of these programmes entail a push to to collect, store, and use the biometrics of individuals as the primary means of establishing and authenticating their identity[4]. While states claim that digital identities lead to efficient delivery of government services, anti-poverty regimes and welfare schemes, or even reduce corruption or help serve national security interests, there are serious concerns with how the systems are designed, and their impact on human rights.

With so much information concentrated within a single database, and within the control of a few actors, digital identity programmes can open up countries to the risks of becoming surveillance states, leading to restrictions on freedom of expression, assembly and association and freedom of movement[5]. Further, risks to privacy that are associated with these programs are too significant to ignore, as people's data can be exploited in ways that can cause serious harm. Digital identity programmes also risk further marginalising people who are already marginalised, leading to social exclusion for many.

Without proper human rights safeguards that are rigorously followed, national identity programmes can be counterproductive to the welfare of the people, violate internationally protected human rights, and undermine cybersecurity. It is imperative that safeguards, both legal and technological, be adopted holistically, and the adoption of one does not preclude the adoption of the others[6].

Countering online hate speech and ethics of algorithms

Online spaces are important avenues for organisation and political participation. People are taking to online spaces more and more to express their dissent on political, social, cultural and economic issues. However, increasingly, these spaces are being hijacked by extremist groups and hate campaigns against religious, ethnic, gender and other minorities have become a common occurrence globally[7]. People are repeatedly targeted for their expression, especially when they seek to challenge religious institutions, undemocratic practices and structures. The

[4] WS17. The Future of Digital Identity and Human Rights https://apps.2019.rigf.asia/submission/proposaldetail?id=305

[5] Ibid

[6] Ibid

[7] Merger 3. Online resistance movements and political organising against and countering hate speech in Asia https://apps.2019.rigf.asia/submission/proposaldetail?id=363

results of hate speech online have also spilled over to offline spaces on many occasions, with many people being killed or their physical safety compromised[8].

One of the biggest challenges in regulating hate speech online is that there is no commonly accepted definition for the term “hate speech” and definitions vary in different jurisdictions and cultures[9]. The is a need for states to do more in regulating hate speech online and for the private sector to be more proactive, consistent and transparent in their moderation of hate speech on their platforms.

There are concerns of free speech and the rights of an individual being curbed due to algorithmic biases when technologies such as AI are used to inspect and remove content on social media. AI algorithms need to be transparent and developed by collaboration of all stakeholders to ensure the protection of Human Rights[10].

II. Safer Internet, Cybersecurity, and Regulation

Growing concerns around issues such as organized disinformation and fake news, hate speech and harassment, online violence and terrorism, organized cybercrimes and, data breaches result in a decrease of trust as well as a wave of state regulations to mitigate the cybersecurity risks. New technologies and militarization of smart lethal weapons and fake attribution threaten to reframe the online environment as a conflict zone which is against the vision of peaceful and development-oriented Internet for human goods.

Legal frameworks and mechanisms

Mapping the legal landscape in each country as it relates to the Internet and civil society can help to outline gaps and ambiguities among existing laws and regulations in relation to international human rights standards. This in turn can highlighting opportunities for advocacy regarding Internet-related law and policy in each country drawing on international human rights standards and best practices[11].

For protecting the privacy of individuals, many APAC countries (such as Indonesia’s proposed law and Australia’s upcoming amendments to the Privacy Act) are now implementing privacy and data protection laws, relying heavily on the GDPR.

An example of regulatory mechanism that can help in protecting human rights online is a pilot project done by iGMENA called Internet Legislation Atlas (ILA) that aims to pinpoint opportunities for improvement and contribute to raising the awareness of concerned

[8] Ibid

[9] Ibid

[10] WS30. The Ethics behind Computing Machines: Raising Awareness of Digital Talents https://apps.2019.rigf.asia/submission/proposaldetail?id=320

[11] WS48. A roadmap for studying ICT laws and building a database for Asia https://apps.2019.rigf.asia/submission/proposaldetail?id=344

stakeholders, and empowering civil society to participate in the Internet policy dialogue in the regional and global level and influence the decision-making process in the local level.

Technical best practices

Evaluating the Cyber Maturity Framework of organizations, including those which provide security for new technologies prior launching and on a regular basis can help improve security by looking at capability areas such as Respond, Identify, Detect and Protect.

Application of technical best practices such as DNSSEC is an important part of the solution as well. However, while we take action on cybersecurity threats on the Internet application layer and within organizations, we cannot fail to protect the core (technical layer). For example, efforts like the Mutually Agreed Norms for Routing Security, provide a clear path for network operators to take towards addressing these routing threats.

Governments should also take initiative to apply technical good practices, to make sure that government critical information is protected and secure safely, for example through the establishment of new Digital Transformation Administrative regulatory body that will oversee important changes in technology, as well as monitoring Government ICT services to meet the standard and security required.

Conventions, wider consultation and multistakeholder roles

It is also important to identify gaps and limitations in governance and questions the illusion of democracy and participation. This is particularly important as it is difficult to prosecute actions done from overseas but only contents that were uploaded locally. The Budapest convention on cybercrime by the Council of Europe is a good example of such International efforts.

At the same time, many states are developing regulations without wider public consultation and many cybersecurity laws have failed to protect the freedom of speech. Further, regulatory Internet isolation, as in Russia and Iran, is of serious issue since it will also affect IXPs and impose their authorities on the routing of global Internet traffic in and out of their respective borders

The private sector has an increasingly important role to play in cybersecurity. An increased understanding and adherence to responsible behavior of tech companies and standardization to secure ICT products supply chain security is part of the collaborative and a multistakeholder approach that must be emphasized.

III. Access and Universality

Internet is an important means for access to information and knowledge, connecting the unconnected to such a global resource remains a fundamental and primary goal. There is evidence that digital divides within national populations are associated with factors such as geography, gender, age, ethnicity and disability[12]. In many cases, these are consistent with structural inequalities in society as a whole, and so with differences in access to other goods and services.

One part of access or the disruption of access: network shutdowns were discussed under the lens of Human Rights in section I, but beyond mere access, how can the quality of access be measured and ensure it is affordable and equitable to all? Concrete efforts of facilitating better access include encouraging more local content and linguistic diversity as well as the adoption of Universal Acceptance (UA) and Internationalized Domain Names (IDN). Capacity building, increasing digital literacy and e-government development are also key components to empower digital citizenship and civil participation.

Adoption of IPv6

With the exponential increase in devices being connected to each other and accessing the Internet, IPv6 addresses will be needed sooner than later as IPv4 addresses run out. Although IPv6 adoption has been delayed partly due to the use of Network Address Translation (NAT), the future points towards IPv6 and early and gradual deployment with a comprehensive plan can increase transition efficiency[13].

Linguistic diversity

According to UNESCO, there are more than 6000 languages worldwide. To have a practical approach to digital language diversity and local content is to adopt policies that encourage local content producers. APAC's sheer language diversity means content should be shaped by its regional languages rather than to rely on content from elsewhere in the world[14]. While this approach may seem overwhelming for some communities, empowering minority groups to produce their own content, and in their own languages, will also help to preserve their culture. In the local context, the creation of new digital content and the digitization of existing content is very important to help increase and improve accessibility. In another aspect, algorithm bias in search engines contributes to a divide based on the language users are searching with.

Universal Acceptance is a part of the bigger picture in ensuring that the Internet's critical infrastructure protocols evolve over time following open standards. Universal Acceptance of Internationalized Domain Names (IDN) and Email Address Internationalization (EAI) for online systems is of priority not only for ensuring Asia Pacific users can utilize their native language to navigate the Internet, but also as an imperative for the continued evolution of the core Internet infrastructure protocols, including the enhancement of scalability (e.g. IPv6), security (e.g. DNSSEC), and multilingual capability (e.g. IDN) for such protocols[15].

[12]Plenary: Digital Accessibility: https://2019.aprigf.asia/docs/digital_access.pdf

[13] WS42. Sharing IPv6 Deployment Experiences among Asia Pacific Countries https://apps.2019.rigf.asia/submission/proposaldetail?id=336

[14] WS35. Language Diversity in Asia-Pacific: Challenges towards Digital Dividends https://apps.2019.rigf.asia/submission/proposaldetail?id=329

[15] Universal Acceptance: Opportunities and Risks for Asia-Pacific https://apps.2019.rigf.asia/submission/proposaldetail?id=364

Accessibility
Integration of more features and facilities (i.e. adding sound into the softwares and websites) so that differently abled persons can access is crucial and the right to accessibility for each person should be respected. In this respect, the design of such softwares and technology need to have accessibility in mind from the creation, and the private sector needs work together with relevant stakeholders to understand the different aspects and criteria for accessibility[16]. Government should have a procurement policy that includes accessibility as a criterion.

Connecting the next billion
About half of the world's population is still offline. People in the unconnected communities generally reside in remote, rural and other hard to reach areas. Due to the low rate of return, the private sector does not find it profitable to connect such communities. At the same time, governments do not always have the funds to build the necessary infrastructure.

Community Networks and other community-based connectivity initiatives could be a viable alternative to traditional large scale commercial networks in providing access to unconnected communities[17]. Slowing growth in voice and Internet connectivity has prompted renewed interest in alternative approaches to addressing the needs of the billions of people in developing countries who still suffer from ineffective communications services due to affordability and coverage limitations. Community Networks, aside from helping to meet worldwide aspirations for universal access, as encapsulated in the Sustainable Development Goals, also provide other advantages including more local control over how the network is used, greater potential for attention to the needs of marginalized groups, retention of more funds within the community and increased potential to foster a sense of agency and empowerment within the community.

Policy and regulatory changes are still needed at the national level. Financial and technical support also need to be granted to Community Networks in the region so they can be on the same playing field as telecoms[18]. This further highlight issues such as the need for increased access to spectrum/telecom data which will contribute to breaking down structural inequalities when it comes to access.

IV. Digital Economy

Digital economy is not just a prospect but an established part of the global economy. Digital tools, technology and services offer great opportunities to learn and earn, especially to the people in underserved areas. However, like other aspects of Internet based services, big companies have an advantage in the provision of such services as well. Local content providers, manufacturers and aspiring companies find it difficult to break into the top tier of business development, due to acquisition and lucrative offers by the tech giants. The Internet

[16] Plenary: Accessibility https://2019.aprigf.asia/docs/digital_access.pdf
[17] WS55. Community Networks – Connecting the Hardest Half https://apps.2019.rigf.asia/submission/proposaldetail?id=352
[18] Ibid

community in Asia-Pacific believes that the digital economy can flourish if the big companies enter into partnerships and collaborations with start-ups, rather than buying them off. Government should also play its role by providing legal data protection to content developers and facilitating conducive environment for Financial technology (FinTechs) through an all-inclusive consultation process[19].

eGovernment for Small Island Developing States (SIDS) in the Digital Economy
While connectivity and accessibility remain an issue for some sections of the Pacific region and a practical challenge is ensuring that their infrastructure will reach the last mile in remote areas, the move towards more positive community-oriented online connections between Pacific governments and their citizens through eGovernment offers new opporunties[20].

eGov websites are able to not only offer a channel of essential services for citizens but also important information about government goals and expectations for tourists and overseas investors. Critical information displayed on such eGov portals should include weather and emergency services for early warnings of climate related events, as well as easier access to health and education/training services for isolated populations.

Transparency and accountability focuses that an eGov site could offer would help to engender greater trust in the government and encourage more citizen engagement with this one-stop-shop for fast and effective delivery of government services. Other benefits which could include opportunities for new employment and entrepreneurial ventures, better health and education as well as knowledge sharing, skills development and capacity building to address national sustainable development goals.

V. Evolving Role of Internet Governance & Multistakeholder Participation

The Internet is a universal tool- raising awareness about its multistakeholder governance so that everyone using the Internet will understand the threats, challenges and economic, cultural and personal empowerment opportunities that come with it is crucial. Internet governance brings all stakeholders to participate at equal footing to discuss policies and build norms[21] for a safer and trusted Internet for everyone.

Working with governments to enhance the policy process
Globally, there has been contrasting discussion between the multistakeholder approach and the multilateral approach, and other hybrid variations. When laws and regulations set by government legal bodies, or norms agreed upon by multistakeholder organizations are done through a transparent engagement process, it reduces friction and becomes receptive

[19] WS23. Big tech everywhere: Is this the future of the Internet?
https://apps.2019.rigf.asia/submission/proposaldetail?id=311
[20] WS37. Is e-Government an effective mechanism for developing economies
https://apps.2019.rigf.asia/submission/proposaldetail?id=331
[21] WS20. Cyber Norms in Asia-Pacific https://apps.2019.rigf.asia/submission/proposaldetail?id=308

concerned parties. Governments depend on parliament members or subject matter experts to comment or endorse new laws and often regulations and bills are being passed through without wider public consultation. Governments need to rethink regulatory processes that include engaging different multistakeholder groups and perspectives. Under the current technology development, public policies are being challenged as the traditional laws and regulations lack understanding and are reactive to these developments. Hence, it is necessary to engage all stakeholders to pay attention to all factors and changes in the Internet governance ecosystem.

Capacity building at the grassroots

The National and Regional Initiatives (NRIs)[22] along with national and regional Schools of Internet Governance (IG) play an important role in capacity building and engagement of youth and underrepresented communities to learn about Internet Governance and contribute to multistakeholder discussions. By taking a holistic approach, NRIs and SIGs could become more effective by coordinating resources to strengthen the capacity of their communities in the Internet governance processes, through knowledge-building and participation support to various IG forums as well as conducting local initiatives. An approach suggested that governments could create incentives for tech companies to allocate budget to capacity building in Internet governance as a part of their social responsibilities.

The growing role of youth

The direction of APrIGF for youth inclusion was best illustrated by a workshop organised by youth, moderated by youth and for youth[23]. Research presented revealed that Asia Pacific youth are growing more aware of Internet Governance and the importance participating in the shaping of the Internet as digital natives and the largest user group. Recommendations underlined the importance of including youth perspectives at every stage of the workshop and agenda setting process.

Two national initiatives that included youth in consultative processes were shared as case studies: In the multistakeholder consultation for the Philippines National ICT Ecosystem Framework, students were part of the consultations from different parts of the country which resulted in the organizing of a national convention for students related to Internet Governance discussions. The Government of Singapore engaged youth through the SG Youth Action Plan to envision the future of Singapore in 2025, which resulted in youth-conducted Internet governance initiatives being a key project that could further integrate youth as a vital stakeholder in the quest for a more inclusive Internet ecosystem.

Collaborating in the multistakeholder ecosystem allows youth to grow in competency and builds their capacity in substantive participation while at the same time strengthening the evolution of Internet governance.

[22] National and Regional Initiatives https://www.intgovforum.org/multilingual/content/igf-regional-and-national-initiatives

[23] WS10 Child-led research on promoting safer internet from children's perspective. 22 young researchers shared their research comprising 8 Chinese cities with a child-centric focus. https://apps.2019.rigf.asia/submission/proposaldetail?id=298