Day 1 Report

ICT landscape and frameworks | 3:00 - 4:30 UTC

Nenden Arum

Session details:

This first session invites participants to explore the regional ICT and digital rights landscape, develop an understanding of key frameworks and structures, and examine the powers and processes that create them. It will also help participants to identify the structures of governance and regulation, as well as recognise the opportunities and challenges that arise across different sectors and countries in South Asia as a result of these regulations.

- Briefly, what are the national and international structures that shape ICT policy and digital rights (standards, treaties, laws, policies etc.);
- What have been the kinds of laws passed in South Asia in relation to ICTs?
- Who are the key stakeholders in ICT governance? What roles do they play in decision making?
- What has been the impact of ICT policies in South Asia on human rights?
- What is a rights-based approach to ICT policy-making? Why is it important?

Session Summary:

This session explores the meaning of ICT and digital rights, and the gaps in the current infrastructure and frameworks. As ICTs began to dominate various aspects including communication, information creation and distribution, markets, governance and civic engagement, it is more important to ensure everyone has access and literacy.

Notes:

Regional ICT Trends in Southeast Asia

ICTs are technologies enabling information creation, communication, storage and distribution. In a decade, ICTs have shifted their purpose from mere communications to transforming the way societies, markets and governance function, even driving the economy forward by playing huge roles in ecommerce and banking operations. The convergence of print media and digital platforms, along with the introduction of mobile connectivity, further transforms civic participation.

Early government initiatives were largely focused on building infrastructures for connectivity and accessibility, especially in rural areas, with the aim of increasing opportunities for all. Such efforts have led to high penetration of the internet in most SEA areas with at least more than 70% of the population, with around 90% in Singapore and Malaysia alone. The region witnessed further widespread digitalisation and digital transformation as triggered by Covid-19, bringing most official and welfare services to the online space.

The expansion of digital technologies has improved access and inclusion among nations, which has opened up opportunities. It also gives the impression of strengthened transparency and accountability for the government, with users able to express their opinions more directly. However, it has also created new harms in forms of misuse of personal data, surveillance, and censorship by the authorities, as well as the market governance dominated by private companies. These issues further increased interest in digital rights, which are exercised and protected in online spaces.

Structures Shaping ICT Framework and Policies

Various national and international frameworks and policies have been installed to regulate the use of ICTs and platforms, recognising governments, private sectors, and civil society as the main stakeholders of the digital landscape. Most countries are recommended to abide by Article 19 of the International Covenant on Civil and Political Rights (ICCPR), which guarantees the right to seek, receive and impart information and ideas across borders. Other mechanisms include:

- UN Business and Human Rights, addressing the private sector’s roles and responsibilities;
- international standards and technical bodies (e.g ITU, IETF);
- treatises such as WSIS, which focuses more on people-centered, community building efforts; and
- Global Digital Impact

Several regional treatises and plans have been implemented, such as ASEAN Digital Masterplan and the ASEAN ICT Masterplans (2015, 2020), with the current focus on the digital economy and digital roadmap using ICT for connecting countries and opportunities for expats, and patchwork of cybercrime, media and surveillance laws. Strong policies on the innovation ecosystem have been developed, in which governments are providing investments on tech development. With the introduction of AI, governments are looking into developing it as infrastructure and as a platform in itself. CSOs aim to propose new workplans with a human rights-based approach for the upcoming ASEAN ICT Masterplan (2026-2030).

At the national level, legislations and regulations have been tabled to address pertinent issues such as ICT connectivity, digital regulation, curbing cybercrime, and ensuring privacy and data protection. Most national frameworks include institutionalising ICT ministries & regulators, cybersecurity agencies, law enforcements, and government-private sector partnerships.

Private sectors’ role in accountability

Some governments, like the Philippines’, have heavy reliance on foreign, commercial social media and a mobile-first internet culture. This makes everyone, especially youth, highly vulnerable to the companies. Because these massive companies prioritize profit and their systems are largely

hidden from users, this reliance acts like a vulnerability amplifier, exposing citizens to constant disinformation, severe privacy violations, and rampant financial fraud.

With these cautions most governments seek efforts to impose strict regulations on the platforms, which can cause a strong tension between both parties. Certain platforms have been blocked as an attempt to curb any production or distribution of content deemed illegal by the state, no matter how much it occupies the platform's space. Users, however, are the most vulnerable as this takes away their freedom of information.

Regardless, SEA is still a valuable market for the private sector and Big Tech companies, promising high usage of its services. Thus, in their interest to maintain the influence, some may form partnerships with the government, or state-produced platforms would take hold of the market.

Digital Identification and Data Privacy as a Means of Surveillance

Governments often mask these regulations as a form of enforcing national security, implying that the digital space itself is a threat. Such attempts include trying to limit information or combat rebellious movements under the justification of cybercrime. Although these legislations seemed to promise safety for the users, more often than not it has been misused for surveillance, with an effort to limit any voices of dissent and citizen's attempts to express their rights online. Even certain rights-based approaches are seen as contradictory to security laws.

Recently, governments are investing in the digitalisation of national identification as a method to increase surveillance. Using biometric identification, its broad purpose is to ensure that all citizens will have access to many government services now made online, and to make certain processes like immigration more efficient.

However, this approach is concerning as the verification process is still unclear. Many of the options available, such as biometric systems, submission and registration of ID, and/or AI verification tools, are still exploitative and inaccurate. Most systems are still vulnerable to data breach and privacy violations, as the technical operations are not fully sophisticated.

Digital identification is often being promoted under the guise of promising safety and 'protecting harm' for selected groups such as youth and children. Recent news in Malaysia stated that children aged 16 and under will be prohibited from having their own social media accounts starting in 2026. It was said that the measure aims to safeguard children from online harm. Digital rights advocates recognise it is more about enforcing registration with MyDigital ID/enforce eKYC verification under the 'protectionist' narrative/restriction-model so that users can be surveilled, persecuted and censored.

This could also harm the right of the children to access information and knowledge, as social media is also where good and current information gets to be shared. It negates young people's agency, as they are already online and able to exercise their own judgement with the right support and info. This is also contradictory in protecting children as Malaysia has yet to outlaw underage marriage.

The SEA region also has a bad record in protecting personal data with no proper security safeguards, as there is constant news on data breach used for frauds and identity theft. While a strict regulation is highly recommended, the law has to be drafted with full interest for the public

good, and not leave any loopholes for otherwise. For example, the Personal Data Protection Act in Indonesia can be misused by officials to hide traces of corruption. Journalists and whistleblowers who have access to such evidence are often being targeted as breaching privacy.

Inequality in access and participation

Despite efforts in ensuring all services are made online for efficiency, there are still persistent inequalities in access and participation. This could be caused by inadequate connectivity infrastructure in certain areas, or an individual's lack of capacity in acquiring a device or digital literacy. This gap further decreases the opportunity to be included or involved in the process of policymaking. For example in Indonesia, all citizens are required to have a digital ID to access certain services. Underprivileged people may not have access to acquire this.

Shrinking of civic space via censorship

The authorities are shifting to not only regulating the infrastructures, but also on regulating the platforms for safety. This includes regulating the content creation and providers, especially with user-generated content (UGC), who may create and distribute harmful content such as misinformation, disinformation, moderation of content distribution and production.

In SEA, social media platforms have become an important political sphere, where it has become an arena for politicians, civil society and other individuals to shape and spread their agenda. The tension between the government and the platforms' interests, along with other factors, further cause persistent digital divide and inequalities.

The question here is on who gets to define which content is deemed illegal? Despite the claims for safety, these regulations are often being misused, with the vague definition and identification of illegal content. Such regulations often breached users' rights for exercising freedom of expression.

With the merger of digital platforms and governance, further enhanced by mobile connectivity, there are no strict boundaries between the online and offline space. With a loose privacy law, non-consensual photos of an individual can be taken and posted online, and can be weaponised against the user.

Rights-Based Approach and Identifying Government's Capacity

CSOs propose a Rights-Based Approach in digital regulations, anchoring in international human rights law and centers equity, inclusion and digital justice. It demands transparency, accountability, and participation from all parties, in which even regular citizens by way of the ICT connection can question policymaking more effectively.

This approach aims to prevent overreach in state surveillance, by recommending an independent monitoring mechanism. It also ensures legality, necessity, and proportionality, to limit unjustified censorship. For example, in the case of the government shutting down a certain group from accessing the internet/social media, thus leading to blocking the platform. This affects all other users who are using that social media for personal and professional use.

The approach also highlights the importance of protecting vulnerable groups and civic spaces by creating safeguards against platform abuse, from other users and from the platform owners itself.

Although the government is seen as the most vital stakeholder that shapes the national ICT landspace, recent engagements have shown that their capacity on ICT is very limited, if not incompetent. They also have a lack of understanding of Rights-Based approach in tech.

In response to the case in Malaysia, rather than banning access and pulling a full shutdown on all platforms, there needs to be an increased focus on digital literacy, safety, and consent on information sharing and production.

However, it is also important to keep in mind that they may not have the intention to take the Rights-Based approach into consideration, limiting CSOs roles in multistakeholder forums.

Recommendations for advocacy, lobbying and educating

By identifying the government's lack of capacity on Rights-Based Approach and digital literacy, CSOs can tap in to play the role in educating them. Can identify a champion among public officials to collaborate with.

Certain political situations can be an entry point for a new political party that speaks closer to the people and is able to touch on digital safety, access and literacy issues. In countries where civil society is quite prominent and has a strong hold on the policy, however, CSOs can advocate to be involved in policymaking.

CSOs should unite and be in solidarity with each other regionally. By working together as a collective, able to put a bigger pressure on Big Tech companies who see SEA as the main market. A good relationship with these companies' local representatives are not sufficient as most of their main operations are outside of SEA and they do not have any power in decision-making. Thus it is stronger for CSOs to work and voice out as a regional collective.

CSOs can also reach out to the youth directly, teaching how open-source platforms work as an alternative.

CSOs should also be prepared to exist and work beyond social media, as we could exist before it.

Key Takeaways:

- ICT governance is shaped by complex national & international structures
- SEA faces recurring patterns of restrictive digital regulation
- Stakeholders hold uneven power in decision-making
- ICT policies deeply affect civic space & human rights
- Rights-based frameworks are essential for a safe, inclusive digital future

---

Access and inclusion | 5:00 - 6:30 UTC

Damar Junairto

Session details:

The focus of this session is to develop participants' understanding of meaningful access and the regulatory frameworks that enable Internet connectivity. It will also invite participants to examine the digital divide, its effects on marginalised groups, and policies and initiatives designed to promote inclusion. This session will further incorporate regional case studies in the region that illustrate how these issues play out in practice, enabling them to connect theoretical perspectives with lived realities.

- What do we mean by meaningful access? (including discussion of access as a right)
- What are the regulatory and policy frameworks that shape internet connectivity in South Asia? What are the gaps?
- What are the challenges to digital inclusion (including the gender digital divide and the importance of an intersectional approach)?
- What are some initiatives or models that could be useful to address issues of access and inclusion (community networks, universal access funds etc.)?

Notes:

The internet is a key enabler for the exercise and enjoyment of many human rights, esp Freedom of Expression (FOE) and Freedom of Information (FOI). However, lack of adequate infrastructure or connectivity leaves behind the poorest communities. The meaning of 'Digital divide' has expanded beyond getting connected. The lack of access creates inequality and no inclusivity means discriminatory for the vulnerable groups.

One of the major policies on internet access for all is the UNHCR Resolution A/HRC/32/L.20 - 27 June 2016, affirming the importance of the promotion and protection of HR over the internet, emphasizing the internet is the right of everyone and must be guaranteed.

Recognising that the world has become more digital, with many life aspects having been dependent on the internet such as seeking information, communicating, and even accessing directory and maps, it is more important for internet access to be granted and acknowledged as human rights. Many of the younger generation have become digital native as the digital environment plays an integral part in their worldhood. With most government and official services now made online, it is even more important for all citizens to have access and be able to navigate any restrictive laws imposed.

Can't escape the internet, enables all rights, the world is more digital, necessary for life, empowering citizenship, alternative spaces, to enjoy new advancement, information transparency, navigate restrictive laws

- Necessary for life: a lot of our life aspects depends on the internet: seeking information, contacting people, access maps

- Empowering citizenship: we do not live in a blank context, we've embedded some cultural roles. We need a platform to defend our rights and be functional.
- Internet access is human rights: people are digital native, with kids growing up with technology. They're shaped by the digital environment in their lifehood, an integral part in their worldhood.

Internet access.

Most SEA nations have National Broadband Plans and Universal Service Obligations/Access Funds (USO/USAF) designed to subsidize connectivity in underserved areas. There are three important components that will ensure the connectivity, which are:

- The process of connecting to the internet, which requires personal devices, landlines and sim cards;
- The ecosystem of the service provider, in which certain websites and connections are subjected to data signalling rates and different internet speeds. Some services can be limited by the subsidisation; and
- The individuals or organisations that are enabled to avail internet services/web-based services

Structural Policies and Frameworks on Internet Access

Many institutions have recognised the importance of ensuring internet access, with the establishment of the UN International Telecommunication Union (ITU).

In SEA, different countries have different provisions and implementations, but all with the acknowledgement that it is vital to increase connectivity for all as ecommerce has become a core market. In Indonesia, support is channeled via BAKTI (Telecommunications and Information Accessibility Agency), in which citizens have the right to question the government if they fail to provide or create any infrastructure for disconnected areas in the country.

In the Philippines, several legislations such as E-commerce Act of 2000, and Free Internet Access in Public Place Act of 2017, and Telecommuting Act of 2018 sanctions free wifi connection for several places. Some public spaces in Jakarta, Indonesia, used to offer free public wifi, but recently these spaces have grown smaller. In other countries like Malaysia, however, there is no explicit act on ensuring connectivity, but rather laws on regulating content and misinformation under the Malaysian CMA 1998.

Recognising Meaningful Access and the Gaps

Mere internet connection is not enough. It is important to recognise what enables a meaningful access, which could be attributed to these three components:

1. Connectivity: Beyond having a simple coverage, many websites and applications now require higher speed. Thus, the connection needs to require reliable 4G/5G speeds but also remain affordable. Consistent daily access should also be guaranteed

2. Hardware: ownership of appropriate devices. Shared access or mobile-only access often limits full economic participation.
3. Empowerment: digital literacy and confidence. The ability to use the internet for creating value, not just consuming content.

Many factors have obstructed all users to acquire such access, such as the lack of government support, digital autonomy, digital literacy, geographical barriers. While the government has made various efforts to build infrastructures in all areas, there are still difficulties in accessing the internet in underdeveloped areas or in areas obstructed by walls or trees, including in the city.

Women in the region are also often found restricting their internet use to specific apps like social media due to a lack of confidence and skills to explore the broader web. In some cases, where ownership of devices is limited, women, especially those who do not have job opportunities in the market, are being restricted as they are not prioritised along with family members who are participating in the market. There needs to be a marked effort to ensure that access is inclusive.

Ultimately, with both the government and private companies/platforms playing a huge role in gatekeeping access, it is imperative for their political will to address such issues and ensure that every community has equal opportunity to access the proper networks.

- “Access to a device and connection alone are not sufficient to meaningfully transform the lives of women and girls” - UN Women Report

Case Studies

- Ciptagelar Village, Indonesia.
  - A community-based internet infrastructure, with collaborations from ISP and ICT companies, schools and other support to provide local Wi-Fi connection to an indigenous village. (link) This effort also improves their digital autonomy, as the village has the unanimous power to decide how much access they want. They can also have this choice that can ultimately be accessible for women and girls. And not all regulatory frameworks that can offer this meaningful process.
  - Comment: “if building the internet is illegal here, then the law in Indonesia only serves the people who have a company or state-owned company.”

- Internet Shutdown - West Papua
  - KOMINFO states that they want to protect the people from the sources of these protests, but indirectly blocks information regarding what is actually happening at West Papua and avoid the spread of information.
  - Internet access is political. It is not about who can afford, but who gets to decide which region is allowed to get connected.

- Digital Curfew - Myanmar.
  - While shutdowns have been happening before the coup, but after the failure of the coup in February 2021, more severe internet shutdowns have been imposed. The blockage of VPN by the military junta is happening in most cities, disabling most people from accessing any available free VPN. Most SIM cards are blocked

from receiving OTP from other applications, so people have difficulties in receiving it. The curfew, which is from 10pm-10am, is also gendered as many women could only get some downtime at that time to get connected to the internet from their work.

- Social Media banning in most Gen Z Protests (2025)
  - Building off from millennials' use of Twitter in earlier digital-led protests, Gen Zs are able to organise quickly online using via TikTok. Governments threaten to ban certain platforms to ensure that no information on the ground can be spread, but also to restrict any FOE.
  - Although the Philippines have yet to impose any social media bans, there are strict regulations on the access towards social media, either limited by the subscription plans of mobile connectivity or domain limitations. The banning or rather the regulation of social media aims to curb addiction, sexual contents and exploitation contents. It also points to the internal company documents that aim to target gaining engagements and profits. There needs to be a balance on implementation for the older generation and younger generation.

- The price of data packages and subscription plans has largely increased, which has caused many people unable to achieve meaningful access.
- New platforms like Discord play a huge role in bringing communities and new demographics together for change. For example, in Nepal, Gen Zs organised on this platform for political change. But what does that look like at a larger scale? What are the guardrails/regulations when we are talking about such movements? How to push private sectors to terms with this context and what they need to do in order for their tech, their tools, to not end up being tools for surveillance etc especially on the street?
  - Discord could pose tensions between formal governance framework and informal platform controls. Such an initiative could be organized with the users autonomy yet still marked under the platform's control. We should analyze the grey line to what extent these formal frameworks (government and platform) ruling could affect this community based space? How should informal actors (the community admins) should act regarding this issue?

Other reflection questions:

- Do we like the idea that the Internet is a public good, so it should be free?
- Who should we hold responsible when there is internet disruption?
- How does internet access intersect with disability rights

Revision #5
Created 18 November 2025 16:40:50 by Cho
Updated 9 December 2025 05:09:52 by Cho