Documentation

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

Day 2 Report

Freedom of expression and privacy | 3:00 - 4:30 UTC

? **Sanhawan Srisod**

Session details:
This session is aimed to explore the laws protecting freedom of expression across the South Asian region, while also examining the restrictions placed on this right within different legal systems. Participants will look closely at laws addressing hate speech, sedition, blasphemy, and defamation in their regional contexts. The session will further provide a brief historical overview of these laws and restrictions, tracing how they continue to surface in both offline and online spaces today.

- Broadly, what are the provisions that cover freedom of expression in international human rights law and national legislation in South Asia?
- Restrictions on FoE - what does international law say, and how does it compare to the kinds of restrictions we see in South Asia (hate speech, sedition, blasphemy, defamation and mis/disinformation etc.)?
- What kinds of laws are being passed in South Asia in relation to freedom of expression online? How does this differ from how FoE is regulated offline?
- What is the role of platforms with respect to freedom of expression online? What impact does the current policy approach towards platforms in South Asia have on FoE online? What needs to change?

Notes:

Introducing International Commission of Jurists (ICJ)

ICJ is an international NGO based in Geneva, consisting of a group of lawyers that aims to promote the rule of law according to human rights standards.

In 2019, ICJ released the report Dictating the Internet: Curtailing Free Expression, Opinion and Information Online in Southeast Asia (2019) which noted a worrying trend on legislations and frameworks regarding regulating the internet. Since the release of the report, there had been no changes, if not worse, in such regulations. In the past 5 years, many laws in SEA countries had shown a chilling impact on FoE, with new laws revolving around regulating AI looking similar to previous cybersecurity laws.

Following the report, ICJ had also released various country-based reports, including Cambodia 2020, Vietnam 2020, Thailand 2021. 30% of the reports highlighted the legal frameworks that were further accelerated to curb the Covid-19 pandemic.

Other reports produced are:

- Singapore’s Online Falsehoods and Manipulation Act 2019 - to what extent it comprises

the human rights principles
- Counterterrorism and Human Rights in Philippines, 2022

ICJ had also issued statements, including on Indonesia's ITE Law revision's threat towards FoE.

Currently, ICJ is working on developing The Global Principles, which looks into existing international law and standards - both UN treaties and regional instruments - and how it should be interpreted, applied, and enforced in the digital space, in the spirit of progressive development. The project looks at various international standards, including criminal law, to regulate the digital challenges that arise especially with the emergence of AI, which has caused rapid changes in tech and digital spaces.

The Global Principles contains 35-37 principles, split into 5 Scopes:

- General Principles
- State obligations
- Corporate responsibilities
- Remedies and Reparations - Recognising the types of harms, the potential remedies and access to acquire the solutions
- Accountability - mainly focusing on an individual's accountability on violations in the data world, and the judiciary oversight that is eligible

The project was first launched in June 2025 and aims to be finalised in mid 2026.
The drafting of the Principles is to be accompanied by advocacy guidance or commentary to ensure that this can be a useful and practical toolkit.

Human Rights Laws on the Online and Digital World

In general, most of the human rights laws were created after WW2 and had no considerations on the digital space at the time. With the evolution of the digital space, the conversation mostly revolves on which human rights laws that are traditionally applied offline could be converted online, as it is more complicated in the latter. With more government services being transferred online, there is a higher urgency for every individual to remain connected in order to gain access to certain rights.

Certain rights that are often being interchanged in both spaces are:

- Freedom of Assembly: could be protected offline, and should be online as well.
- Right to Health: Revolves around access to the best quality of healthcare service. Many services are now utilising telemedicine platforms and digital health options.
- Right to Development - Indicates the protection of natural resources and economic development. However, it is more vague and ambiguous online
- Freedom of Opinion and Expression - should be protected
- Freedom of thought, conscience, and religion - UN Expert confirmed that it should be protected
- Right to Privacy - definite.

The pandemic spurred several other new trends as many services were forced to be online:

- Right to standard of living/access to food
- Right to education
- Right to work
- Rights to equality, equal protection of the law, and discrimination

International Instruments on Freedom of Expression: ICCPR

Most SEA countries are part of the International Covenant on Civil and Party Rights (ICCPR). Countries that do not officially rectify this are still bound to the ICCPR's general rules and practice.

Customary international law - 'international custom, as evidence of a general practice accepted as law', which means there must be a general and consistent practice by States, while there an agreement exists among them that the practice is acceptable. This also applies to certain laws that are not necessarily rectified by all, but most countries should abide by it. One of the most famous instruments that has achieved this is the Universal Declaration of Human Rights, including FoE. However, it is important to bear in mind that the UDHR is an old instrument.

- Article 13 - right to freedom of movement

Freedom of Expression is based on Article 19 of ICCPR.

1. Everyone shall have the right to hold opinions without interference
2. Everyone shall have the right to freedom of expression; include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, through any other media of his choice.

In 2011, the UN released a General Comment NO.34 to the Article 19, which includes FoE protection online via "protecting in all online and audio-visual form" .

Requirements for restrictions of human rights online

There are three conditions where restrictions may occur:

- Normal times - human rights treaties allow certain limitations on human rights
  - Restrictions under Art 19 of the ICCPR

    1. "... subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) for respect of the rights or reputations of others; (b) for the protection of national security or of public order (ordre public); or of public health or morals"
    2. "Must conform to the strict tests of necessity and proportionality"

- Restrictions under Art 20 of the ICCPR
  1. "Any propaganda for war shall be prohibited by law."
  2. "Any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law."
- Emergency situations that threaten the life of the national (e.g major natural disasters such as severe floods or earthquakes; public health emergencies such as Covid-19)
- Wartime

Non-compliance trend - patterns of abuse reflected in laws during normal time

Referring to the FoE restrictions under Article 19 of ICCPR:

1. "... subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) for respect of the rights or reputations of others; (b) for the protection

of national security or of public order (ordre public); or of public health or morals”
2. “Must conform to the strict tests of necessity and proportionality"

To understand if the restriction is legitimate, one should conduct the 4-part test (to prescribe restrictions):

- **Legality:** prescribed by law while ensuring that there are clarity in its regulations
- **Legitimate purposes**: pursue a purpose recognised as legitimate under human rights treaties
- **Necessity:** necessary for achieving that purpose (because there are not other human rights framing to conduct it)
- **Proportionality:** proportionate (ensure that the law is on equal level with the harm. For example, the law of defamation should not entail imprisonment or criminal penalties)
- + non-discriminatory

Whereas restrictions under Art 20 of the ICCPR states that**:**

1. “Any propaganda for war shall be prohibited by law.”
2. “Any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law.”

To define incitement, a 6-part test called **Rabat Plan of Actions** is used for expressions considered as criminal offences:

- Context
- Speaker
- Intent
- Content and form
- Extent of speech act
- Likelihood and imminence

In Meta, one can file a complaint to The Oversight Board who will look based on the Rabat Plan of Actions. One specific case is that the Oversight Board has overturned Meta’s decision to leave up a video of the Cambodian Prime Minister’s threat towards his political opposition.

Laws with FoE Restrictions and Case Studies

Laws that commonly restrict FOE even in the online sphere are :

- Laws protecting reputation (defamation)
- Laws on national security and public order
- Laws regulating online information
- Laws aimed at controlling the spread of ‘disinformation’
- Laws regulating telecommunication

The common theme is that most laws offer vague and overly broad provisions such as ‘false information’ (against Legality). Some laws also fail to clarify terms such as “public order” “national security” (legality & legitimate aim). This poses a question on who gets to define false information, and against whom. However, despite the ambiguity, such laws would impose severe penalties such as imprisonment e.g. some acts under A20 (Proportionality).

One participant mentioned that “these laws in the region are often colonial era laws that do not get updated with any recent human rights development or recommendations, which puts a challenge as these are systems that were never designed with the realities of the region and today’s world.” The slow or refusal of improving such laws in accordance with recent updates and research also creates tension that often jeopardises civil society and actual public interest.

Another pointed out that such ambiguous provisions, more often than not, diminishes public confidence in the performance of the government.

Case study 1: Computer-Related Crime Act (2007) - Section 14 - Thailand
Vague and broad legality and legitimate aims: The definition of ‘national security’, ‘public safety’, ‘economic safety’ is highly dependant on the authority

Instances where this law has been used:

- A BBC journalist faces defamation charges in Thailand, in which the ‘National security’ could be used even on a municipal level.
- A HRD who posted an incorrect location for a mosque, and quickly corrected it in 30 minutes. But still gets charged as the post was detected by the military.
- Entertainers, media, or songs that criticises the authority

While most of these cases are often dropped after judiciary oversight, the affected individual(s) and their resources are still largely impacted.

Case Study 2: Protection from Online Falsehoods and Manipulation Act 2019 - Singapore
Vague and broad legitimate aims: Lack of definition on the ‘false statement of fact’; security; public health, public tranquility, public finances, friendly relations with other countries, influence the outcome of an election

Case Study 3: Article 27 (Philippines)
Contents against propriety / contents of affronts and/or defamation

Case Study 4: Cross-border jurisdiction

Recently an Australian journalist was recently indicted for alleged Malaysian government defamation following a complaint from the Malaysian MCMC, and was filed a complaint via the Malaysian Embassy in Thailand. The question is which jurisdiction’s laws apply when the alleged “defamation” originates from published content accessible across borders.

It is worth noting that Defamation is a common weapon in the political sphere. This tactic suppresses any political opinion, which is used either on opposing political actors or even on common public individuals. This causes a decrease in confidence among the public to express their opinions.

Restrictions during Emergency Situations or Wartime
Access to human rights in the digital space during natural disasters can be disrupted by the infrastructure damages caused by the occurrence, which could lead to users having lack of access to important updates and information. It would also cause low capacity on getting access to support and resources.

However, certain states have conducted drastic measures such as internet shutdowns, disrupting mobile signals, or platform blockings to reduce any coverage on potential protests, dissent or their neglect towards counteractive policies.

Some rights may be derogated from, but only if the measures:

- Strictly required by the exigencies of the situation exceptional and temporary, and it should be removed once the situation has improved
- Not inconsistent with the State's other obligations under international law
- Do not involve discrimination

For example, in Myanmar: The Telecommunication Law 2013 contains a provision "For the duration of the public emergency, direct any licence holder to suspend telecommunications". This could create legitimate aim concerns as the "duration" and the "public emergency" are not well-defined, and it could be extended even if the conditions have improved.

Concluding thoughts:
Troubling State responses include:

1. Enacting overbroad criminal laws
2. Introducing laws that lack precise definition
3. Granting unchecked

Corporate Responsibilities:
UN Guiding Principles on Business and Human Rights (UNGPs)

- Advertisement-driven business model - profit driven, often push posts that incite hate and bigotry for high engagement.
  - Myanmar: Facebook systems promoted violence against Rohingya
  - Thai influencer profiting from the Border conflict with Cambodia
- Inadequate content moderation
  - Meta is ending their third-party fact checking mechanism which involves hiring human fact checkers, to move to the community note model. The latter could run into some risks as there are no proper guidelines on doing so, with the vague morality across the public
- Opaque policies and practices
- Lack of accountability

Tech companies shall:

1. Review their business models
2. Content moderation practices shall be consistent and sufficiently resourced, with human-in-the-loop safeguards
3. Adopt clear and easily accessible policies aligned with IHRL
4. Conduct regular human rights impact assessments
5. Publicly report on government requests
6. Establish effective remedy mechanisms for wrongful takedowns

Reflection Questions:

1. Most of the issues revolve around the definitions of the term being used. Would it be helpful if the terms are further expanded (thus binding) in law, or would that result in further complications?

2. Who has the authority to define such terms? What avenues needed to imagine and realise alternative solutions beyond the agendas set by big tech, the state and other powerful forces?
3. Cross-border jurisdiction: recently an Australian journalist was recently indicted for alleged Malaysian government defamation following a complaint from the MCMC, and was filed a complaint via Malaysian Embassy in Thailand. Which jurisdiction's laws apply when the alleged "defamation" originates from published content accessible across borders?

- https://www.ifj.org/media-centre/news/detail/category/press-releases/article/thailand-australian-journalist-indicted-for-alleged-malaysian-government-defamation

---

Privacy, surveillance and data protection | 5:00 - 6:30 UTC

? **Jam Jacob**

Session details:
In this session, participants will learn to examine the different facets of individual privacy in the digital age and the regulations designed to protect these rights. They will investigate the impact of emerging technologies on decisional privacy by considering the various forms of surveillance currently deployed in society alongside the enabling legal frameworks. This session will further focus on the rise of surveillance-related policies and their implications for the protection and promotion of digital rights.

- What is privacy in the digital age and why is it important?
- What are the ways in which the internet and other digital technologies are being used to infringe privacy and engage in surveillance?
- What are the legal and regulatory frameworks in south Asia that protect privacy, including data protection laws? What are the challenges and gaps?
- What are the ways in which legal frameworks in South Asia are being used to enable surveillance?
- What is the impact of such policies on freedom of expression, assembly and association and other rights, esp for marginalised groups?

Notes:

Objective:

- Learn to examine the different facets of privacy in the digital age and the regulations designed to protect these rights
- Investigate the impact of emerging tech on privacy and other digital rights by considering the various forms of surveillance deployed today alongside the enabling legal frameworks

Privacy and Data protection

Definition of Privacy:

As far as privacy is concerned, it's difficult to come up with a universally accepted definition due to many factors that influence the individual and society's notion of privacy.

European Court of Human Rights, Niemietz v Germany (1992) stated that the notion of private life is a broad one, not susceptible to exhaustive definition.

The first definition on privacy was by the right to privacy was first defined as 'the right to be le(f)t alone' (Warren and Brandeis, 1890 Harvard Law article), which is the most cherished of freedoms in a democracy.

Participants were asked to define their understanding of privacy, which includes:

- Control over personal information, including location and online activities, and the power to decide who can access your data and how it's used
- Our authority and independency to protect essential data and information related to interests and rights
- Right to decide who has access to us, to be left alone, and how these terms can be fluid and dynamic to fit an individual's needs
- Ability to control what to share, with whom, and under what conditions
- With the rise of AI and LLM, many platforms have manufactured our consent to feed our information and data to their LLM processes, and it is difficult to opt out. Many BigTech companies complicate the processes by hiding their privacy settings.

Right to privacy:

The right to privacy is commonly understood as physical space free from interruption, intrusion or embarrassment, or accountability. There is an interest in human personality; it protects independence, dignity and integrity.

Previously, many legislations aimed to prevent people from invading physical and information privacy. But as technology advances, the line of privacy becomes blurred, along with its legitimacy. For example, prior to the heavy use of the digital space, trespassing physical properties and accessing confidential documents were seen as invasive. However, although wire-tapping phones or phonelines are inherently intrusive techniques, they have played huge roles in revealing and uncovering some important conversations and information.

Our intricate relationship with technology needs further prodding, especially in defining the boundaries, as "Privacy in an age of primitive technology was largely a function of inefficiencies in technology in monitoring and searching." (Jeffrey Rosen).

Aspects of Privacy

- Privacy of communications - emails, messages and telecommunications
- Bodily privacy - from certain invasive procedures, physical space. For instance, airport scannings could lead to feeling discomfort, hence the need for some regulations on the procedure.
- Territorial privacy - Rules governing the proper conduct on physical surveillance such as by private investigators, law enforcement agencies, CCTV cameras and its locations (in restrooms or rental homes)
- Informational privacy

Example: One participant shared that privacy of communications and informational privacy could affect health and reproductive health centers, as affected women may need access to get their right to decisionmaking on accessing the contraceptives needed.

International Policy Landscape on Privacy

There are two important international instruments on privacy, which are:

1948 Universal Declaration of Human Rights, Article 12 (UDHR is a law, not a treaty. Not necessarily binding):

- “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”

1966 International Covenant for Civil and Political Rights, Article 17: a treaty, binding

- “No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
- Everyone has the right to the protection of the law against such interference or attacks.

ICCPR Signed: Cambodia, Philippines
ICCPR Ratified: Cambodia, Indonesia, Laos, PH, Thailand, Timor Leste, Vietnam
Not signed nor ratified: Brunei, Malaysia, Myanmar, Singapore

- Malaysia - goes against national constitution that protects the Malay Majority rights

Other international laws can be found here (slide 11).

Permitted Limitations:
The right to privacy is not absolute, and the infringements/intrusions must not be arbitrary or unlawful. It should be tested against these 4-part tests:

1. Must have a legal basis
2. Must have a legitimate aim (national security, public order, public health, morals)
3. Necessary/necessity
4. Respect the principle of equality/proportionality

For example, if the surveillance is conducted according to selected legal basis, then it is permitted. The surveillance method could also be proven necessary if the information could not be retrieved through other means.

Constitutional Guarantees listed on slide 13.

Comparing UDHR and Vietnam’s constitution, which shares the same principles:

UDHR	**Vietnam**
“No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”	Everyone is entitled to the inviolability of personal privacy, personal secrecy and familial secrecy and has the right to protect his or her honour and prestige. Information regarding personal privacy, personal secrecy and familial secrecy is safely protected by the law. Everyone enjoys the secrecy of correspondence, telephone conversations, telegrams, and other forms of exchange of personal information. No one is illegally allowed to open, control, and confiscate others’ correspondence, telephone conversations, telegrams, and other forms of exchange of personal information.

Data Protection
This means the individual has control over one's personal data.

Data protection vs data privacy: In many cases, these terms have been used interchangeably. There are many arguments on the perceived distinction between these two concepts, and the closest that is suggested by the RP is by looking where the user is coming from. If you are the rights holder of your own information, you may call it Data Privacy.

But if the individual is acting as a person who has authority over a number of data (Controller, Duty Bearer), then it would be referred to as Data Protection.

In the Philippines, the Data Privacy Act 2012 is mostly based on the EU Data Protection Directive 1988 (the predecessor of GDPR).

Data protection vs information security: while data protection looks at personal and individual data, information security refers to a larger scope of data and information. This includes data that are not necessarily considered under privacy (including weather, economy, etc).

- Tasks under Information Security:
  - Ensure the confidentiality and backup copies are still accessible and available
  - To ensure the information remains accurate, up-to-date, integrity is intact
- Tasks under Data Protection/Privacy:
  - Similar as IO, but extra concerns with regards to the rights of the data subject, privacy principles, security/safeguarding from intrusions

The earliest discussion on information technology occurs in the 1960s, coinciding with the development of computers and faster processing of data. States began to worry that these systems, if left unchecked, would lead to harm.

- Hesse, Germany - first known modern data protection law

International Policy Landscapes on Data Protection:

- Fair Information Practices Principles (1973)
- OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (1980, 2013) - Most laws follow this guideline
- COE's Convention for the Protection of Individuals with regard to the Automatic Processing of Data [No. 108+] (1981, 2001)
- EU Directive on Data Protection (1995) - influenced the Philippines
- APEC Privacy Framework (2005, 2015) - has less influence compared to EU Directive
- EU General Data Protection Regulation (2016) - most influential and regarded as the standard of data protection

Slide 16-17, which includes the SEA countries' Data Protection Laws and their year of enactment:

* Myanmar’s Data Protection Regulations took reference from their Cybersecurity Laws
** Only Cambodia has no Data Protection Law.
*** Zana mentioned: Malaysia’s Data Privacy Law is still limited to PDPA that only regulates how personal data is handled by organisations in commercial transactions, and does not effectively address other aspects such as doxxing. Even when doxxing falls under laws such as PDPA + CMA + CCA, these laws do not expressly provide proper avenues to address these crimes because CMA and CCA were enacted before cybercrimes became more relevant.

Regional Laws and Mechanisms:

- ASEAN Framework on Personal Data Protection (2016) - high level principles that are supposed to guide ASEAN members, such as consent, access, security, safeguards over borders
  - To build/facilitate transferability across regional legislations
- ASEAN Digital Data Governance Framework (2018)

    - Data protection, data flow, security
- ASEAN Model Contractual Clauses for Cross-Border Data Flows (2021)
    - Support a trusted harmonized ecosystem that enables a robust regional digital system. Cross-border data transfer is discouraged, but it is allowed according to certain requirements. These are contract templates that organisations can use to offer enough protection for the data transfer within ASEAN
- ASEAN Data Management Framework (2021)
- APEC Privacy Framework (2004, 2015)
- Global CBPR Forum (2023) - builds upon APEC's certification on cross-border data system

One participant pointed out that the current geopolitical context also shows that such data is also being used for international trade. As part of the tariff negotiations with the US, the Indonesian government initiated that both countries will finalise commitments to digital trade, services and investment, including the ability to transfer personal data out of its territory to the US. This is their attempt to navigate around the EU's GDPR.

Emerging Tech, Enabling Laws and Impact on Digital Rights

Recall: privacy-technology relationship

In the 21st century, we witnessed rapid development in tech capacity to intercept and process communications; major drop in data retention costs. There are various mechanisms in trying to protect data via encryption.

These are the list of emerging tech and laws that are troubling:

- AI-enhanced CCTV & facial recognition in 'safe city' projects
    - Example: Myanmar, Vietnam, Thailand, Singapore
- Commercial spyware deployed by law enforcement and other government agents
    - Academics, civil society in other places are being surveilled by the Pegasus tool, which enables users from another country or region to access their files
    - Example: Thailand
- Social media monitoring & data-access rules, including using AI tools
    - Vietnam - a law that requires platforms to monitor social media content and store data collected from the citizens within the jurisdiction of the government
    - Many other countries are beginning to take note of this. This could also lead to privacy and information leak
- SIM registration & large-scale identity databases, dangerous with the constant data leaks to companies, and intrusive surveillance by governments
    - Most countries in SEA

Examples of Enabling Laws: Domestic (slide 22-25)

There are laws that facilitate the usage of these technologies. These slides looked at Myanmar, Indonesia, Malaysia and the Philippines.

Myanmar

- Cyber Security Law (2013, 2021)
    - Requires digital platforms to retain data for 3 years and turn it over upon mere request by any military-controlled authority
    - Ideally, state governments need to apply to request.

    - Requires digital platforms to censor content deemed as disrupting the “peace”, spreading “rumours”, inciting “terrorism”
- Electronic Transactions Law (2004, 2013, 2021)
    - Enables online surveillance and monitoring (eg monitor comms, track electronic transactions, collect data from ISPs and platforms, access user accounts)

Examples of Enabling Laws: International

- Cybercrime

Impact of Surveillance-Enabling Laws

- Erosion of privacy and data protection rights
- Chilling effect on freedom of expression
- Targeting of HR defenders, opposition, and minorities
- Restrictions on freedom of association & assembly
- Enabling of censorship and information control
- Algorithmic or AI-enabled discrimination
- Increased vulnerability to cybercrime due to mass data collection

Day 3 Report

(To be updated)