□□ Documentation

- Day 1 Report
- Day 2 Report
- Day 3 Report

Day 1 Report

ICT landscape and frameworks | 5:00 - 6:30 UTC

Apar Gupta

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?

Key Themes from the presentation:

Platform Governance

In the past decade, there has been an increased number of internet connections in India, with the current record of 970M+ internet connections, following an increase of 300-400M users on Instagram, Youtube and WhatsApp. Access to data per individual is unequal due to socioeconomic status, with some owning multiple connections, and some without any access.

As these platforms are now core public infrastructure for speech, news and association, they also govern the visibility on who is heard, silenced, and how information travels. State power further increasingly exercised their governance through the platforms, via specific tactics like notice-and-takedown, blocking, and shadow banning. However, there is a lack of transparency on these rules and implementations on censorship. Such governance choices affect civil society and social movements including elections, protects, minority speeches and journalistic investigations.

Core Concepts:

- An Intermediary is an entity that carry, host or process third-party content (ISPs, social media, messaging apps, cloud, CDNs) which allows the user to use the internet

- Intermediary Liability (IL) : when and how the intermediary is legally responsible for user-generated content and is liable for prosecution under national law. Due to the volume of data hosted by the third parties, they are not required by law to conduct censorship, but to be a safe harbor.
- Safe Harbor: Based on Section 79 of the IT Act 2000, conditional immunity for intermediaries if they meet due diligence and procedural requirements, such as having grievance officers. The rationale is to protect innovation and freedom for expression while allowing redress for genuine harm. Intermediaries can be passive conduits by receiving orders by the government to remove any illegal content or provide the user data to the authority.
- Design tension: too much immunity -> impunity; too little -> over removal and private censorship. May affect advocacy on civil liberties, protests revolving around vulnerable groups, whistleblowers.

The Indian Framework: From Safe Harbor to Delegated Censorship

- The IT 2000 is a law modelled after UNCITRAL Model Law on Electronic Commerce (1996), responding to the emergence of the internet in 1996. It contains Section 79, in which intermediaries are not liable for third party content, and enjoys safe harbor if they meet due diligence and procedural requirements, which indicates that they are expected to take down content deemed unlawful or illegal on its own without any interference by the government.
- Due to the high number of users, they need to shift to proactive gatekeeper, which requires a higher level of due diligence on traceability (identifying user), automated content moderation, and “significant intermediary duties”.
- After a procedural change on IT Rule 3(1)(d) in 2021, censorship is being delegated to the platforms. Traceability mandate would require a significant intermediary. Eg any intermediary with above 5M users essentially needs to fingerprint all encrypted messages sent with the identity of the person. The companies will store the user data.
- Executive rule-making (blocking content, content takedown rules) has expanded obligations without full parliamentary debate
- The ambit of IL, which was initially for messaging platforms and apps, has been extended to streaming platforms such as Netflix, Amazon Prime, Hulu and online news platforms such as digital newspapers and magazine articles.
- Social media companies began to comply more aggressively to avoid any criminal risk, or protect user rights and risk retaliation, to maintain a market in countries with more restrictive laws
- Result: Legal uncertainty, forum shopping, and a gradual erosion of the original safe harbor bargain

Censorship

- Government orders for censorship are mostly issued in secret, in which the user has no knowledge on which post or information is deemed unlawful, or weak reason. This restricts any opportunities for meaningful judicial or public scrutiny, impacts access to justice and violates their freedom of expression (FOE).

    - In India, the freedom of expression (FOE) includes the right to receive information. It is not just an injury to the person affected by the censorship, but to the public interest
- Overboard terms that are being used (decency, public order, national security), enable discretionary and viewpoint-discriminatory takedowns. The laws by the government are usually well defined due to the basis of power on the public, in comparison to a private company. The content moderation terms can also be used for government censorship.
- Platforms tend to over-comply, especially on ‘borderline’ speech, leading to silencing dissent, satire, and investigative journalism.
- Marginalised communities, independent media and opposition voices bear the heaviest burden of opaque content governance, as they are afraid of sharing their opinions
- Lack of transparency and remedy, interests regarding rule of law in the country vs the private company’s interests, with the users’ rights being bargained

Towards Rights-Respecting Platform Governance

- Anchor all platform rules in constitutional standards of legality, necessity, and proportionality
- Clear, narrowly tailored statutes; limit overbroad delegated legislation (IT Rules 2000 - amendment to give the government the power to censor anything that is against the nation.
- Protect and modernise safe harbor: liability only after due process, specific notice
- Mandatory transparency: public dashboards on government orders, detailed takedown notices
- Independent oversight and multi-stakeholder processes (civil society, technologists, affected communities) in drafting rules
- Guiding principle: platforms should be accountable, but not converted into privatised censors to the state

Notes from the discussion:

Government initiatives and regulations, safe harbor framework

What has changed in how the government looks at technology and the shift in the last 7 years or so?

The large growth of telecommunication infrastructure prompts a high interest in regulation on the content and type of technologies. As such, the Indian government has been using the Safe Harbor framework as a principle regulation, whereas there’s a global movement for deregulation to increase more innovation and more private industries to thrive.

The Safe Harbor framework offers the ability of the state to not to bring a lot of regulations to operate your business, but still allows the government to fasten a liability on a private company that is required to obey any content takedown requests. While it may not be the best, it is still important for this framework to be protected.

The Digital India Act plays a large role in pushing for digitisation, and yet there are no clear statutory provisions. There are ‘guardrails’ acting through executive notification but there are no fully fleshed out regulations unlike in the EU. pushing for the digitisation of every information, with ‘guardrails’ through executive notification.

How do we balance states' use of broad-based language to allow regulation of emerging technology and the chilling effect that it produces, if we maintain the ‘Safe Harbor’ framework? (especially to curb Big Tech)

It is important to see and frame the platforms as businesses that serve their primary interest in gathering data for private corporations, and are no longer acting as passive intermediaries. Many problems arise when the platforms have full control on the operations and content distribution.

The issue of broad-based language is due to the larger Rule of Law problem. It has been affected because the constitutional frameworks and the institutions were largely captured by the elites and legalities protests. Even that has been shifted by global populism.

I would double down on the transparency commitment, because at the very least it should allow researchers, academics, CSOs to know more on the basis of the knowledge of public pressure’s outcomes.

Q: What other infrastructure regulations beyond online platforms that we should look out for? And how do we see that impacting rights in terms of the current thinking? What are the trends happening in the region, and what should we prepare in order to push for rights?

It is important to acknowledge that many issues are dominated and steered by technology.

- Licensing and governing telecom and internet providers. In India, the legislation governing telecommunications has changed from the Telegraph Act to the Telecommunications Act, in which the government gets to license who gets to operate the telecom services and especially on running the internet services in the country. While the government is seen as a custodian to the spectrum of the services, this severely serves the government for a number of reasons:
  - telecom companies are expected to give shares and equal service to all the networks in the region;
  - more censorship mechanisms such as blocking certain websites, shutting down the internet, net-neutrality, and filtering mechanisms;
  - regulations on hosting and cloud providers, which impacts users’ digital rights to privacy. There’s a default retention on verifying their identity and where do they connect to.
- Technical obstructions in smartphones, such as certain operating system standards and updates are required for certain apps to work.
- The Biometric system Aadhar, which now requires accessing an application to obtain social benefits such as pensions, government support, and more. One of the many drawbacks is the disparity of access for all citizens especially for those who do not own a

device.

Platform regulations and content moderation

Content moderation that was once supported by thousands of workers across the Global South has been dismantled as major platforms cut costs and left a gap for context-sensitive moderation especially when it comes to non-English content. Also in extension it also has effects on information integrity. How do the regulations structure navigate this in a way that is rights-based regulatory models that balance accountability with freedom of expression?

As the platforms have the power to control the visibility of content based on their own interests, it is more difficult to see where the line is drawn, what kind of information they would deliver to the users, with the intent to prolong the usage time. Content moderation is important but it alone does not address or fix the issues as fascism and populism that could contribute to the platforms' initiatives.

Content moderation systems in the Global South which are used to mitigate harm may cause extreme polarisation by amplifying polarising opinions to get more engagement.

Certain issues could also be degraded or desensitised over time, re: Palestine.

Some platforms like Signal would follow human rights principles to a certain degree. Ultimately, there needs to be a shift of thinking and mindset to distribute on diverse platforms, rather than being tied to one certain platform.

Do you think it is useful to compare the models of state control over these platforms and to information flow particularly from across border (eg. banning accounts of users from other countries from view within this country) to Digital Right Management (DRM) 20 years ago. Media companies pushed tech companies to create and impose DRM tech on everything and recreate the control they had over physical world media in digital spaces, then a decade later became even more controlling than the physical world was. Do you see parallels? We also see strange invasions of digital privacy hidden within tax law. Do you think this kind of sideways attack on digital privacy and other digital rights are harder to fight?

Certain tech industries may have also broken the DRM. Eg Google Books who scanned every publication and went against intellectual property. We need to acknowledge the distinction between business concerns and tech companies, in which DRM is being bundled with cheap data and subscription services.

However, piracy is also on the rise as users are looking for content not offered.

The control which tech companies have on people today is immense. It's not only a strategy of locking people in their platforms, but it's also the ability of larger techs investing in smaller start ups and venture capitals, monopolising any new services. There's a high amount of control among 15-20 companies on our technology, with the current AI companies becoming more concentrated

with the perceived value.

Alternative Strategies For a Safe, Accessible and Rights-Affirming Access

Between deregulation by neoliberal privatisation and regulation by the government, what should be the solution to balance the rights-based regulatory model?

The government is expected to serve the public and constitutional interests. Unfortunately, the global trend of playing by the Rule of Law creates a tension in the relationship between the larger government's interests and individual officials who tend to play towards their own interests, which is conducted without any transparency.

There needs to be a full institutionalised regulatory framework, with regulators, that is insulated and autonomous from the political space so that the expertise can grow and develop their own mandate. That regulatory body of large transnational companies has to be in the public domain for public scrutiny and access, as most large private companies are not necessarily champions of free expression. Similar to the government, it's good to have that tension.

The internet is historically different as there are global efforts to ensure multi-stakeholder governance can be conducted. How is this model adopted for the internet and why does it need to find a place at the national level and what are the challenges in the countries in our regions?

Certain multilateral processes around internet governance are available (e.g. UN IGF) to acknowledge recommendations from civil society and other stakeholders, giving them the opportunity to shape the agenda or provide any feedback on themes and decisions to be made. However, most states would opt for state-centric multilateral approaches due to distrust of civil society.

What do alternative models of ownership, development, and innovation look like - models that build community-owned or decentralised pockets of the internet that challenge extractivist and capitalist business models?

And in contexts where accountability mechanisms are failing because states themselves are perpetrators of digital repression and violence, what strategies or governance frameworks could support these alternatives to remain safe, accessible, and rights-affirming?

- There are workshops done on reimagining the technology and relationship with it, and the various exercises have produced poetry, visual art, and mixed media to reconnect with their humanity and reality beyond the internet.
- Worker cooperatives, feminist-guided platforms and alternative tech platforms can be done, and it is important to have legislative frameworks to shape them. These cooperatives may have issues such as funding support, governance structures and their integration of social functions. As reform initiatives may be decadent and vis-a-vis the

current policies and authorities in place. One movement we can learn from is the labour movement, in which we see with the unionisation of gig workers, gig workers' relationship with the platforms.
- There needs to be a range of political activation among people to make them understand their choices politically, in which activists could be more proactive in setting the agenda rather than reacting to how tech governs one’s life. For example, a person who does not own a smart phone can still be aware of how the smartphone can affect their choices.
- We can use aspirational politics, in which it is not present in SA. The public at large isn't aware of how technology affects them in a deep way, unless a politician informs them.
- The tech bubble is also breaking as we learn how certain environmentalists and gender rights movements distribute their message across these platforms against the algorithm.

Access and inclusion | 7:00 - 8:30 UTC

□□ Nandini Chami

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.)?

Key points from the presentation:

Mentimeter:

1. Addressing the divides in meaningful access will ensure digital inclusion
    1. Not sure: We are battling other issues such as poverty, fascism, etc
2. South Asian economies have other priorities to address before the quest for AI transformation
    1. I disagree: Does not think we should look at other priorities as distinct, it can be fought in parallel with each other when these issues are structurally interconnected.
3. In South Asia, what is the biggest challenge to effecting digital inclusion?

1. Political will, poverty and digital literacy, knowledge

SA is home to 2 billion people, and has emerged as one of the world's fastest-growing regions during the first two decades of the 21st century demonstrated by GDP growth rates. The second date experienced higher economic growth in Bangladesh and India, with jobs affected by AI development.

Coverage gap: Afghanistan and Pakistan have a coverage gap of over 10%. Usage gap, percentage of the population who live within the footprint of a broadband network but not using internet: 42%

Mobile internet subscribers: the number of unique users that have used internet services on a mobile device that they own or have primary use of at the end of the year

To take note that the connection is available because of the subscription, but not necessarily on actual usage.

South Asia's mobile use landscape

Gaps in affordability - SA has a huge gap on gender employability.

Gaps in usage - while there is no significant rural-urban gap, but men

Gender divide: Typically, headlines tend to lean towards women's usage on the internet. Often hear about mobile bans by the local government agencies. Even more than overt gatekeeping, there's systemic and patriarchal barriers by patriarchal gender norms.

Women use it to speak to family; using cheaper phone thus access is limited; digital skills and time constraints

Young women, aged 18-25, how they navigate household patriarchies to allow their access and use of the internet. The participants of the FGD described the approach as 'Cinderella' and playing an angel image - uses social media but rarely posts on it, rarely accepts requests from male users, and tries to balance perceptions and performs how the family should be portrayed.

Online GBV on women and minorities - especially on the rise of synthetic media. Study by Equality Now, 2025. Indian law enforcement agencies describe the process of getting social media companies to remove abusive content (eg 'revenge porn') as "opaque, resource-intensive, inconsistent and often ineffective"

Often ends up policing and surveilling women, and suppresses women's self-expression and sexual expression

Access is NOT equal to digital inclusion on empowering terms

- Alison Gillwald, : The connectivity paradox - the internet is not an automatic enabling pathways to development
  - Advanced technologies are layered over underlying foundational infrastructures

    - significant disparity between those who have technical and financial resources to use the internet actively and productively, vs ‘passive’, ‘barely’ online users using tiny bits of data communicate intermittently
- R.Heeks: All inclusion is not entirely empowering, ‘adverse digital incorporation’.
    - Inclusion in a digital system that enables a more-advantaged group to extract disproportionate value front eh work and resource of the less-advantaged
    - The growing pace of digitalisation during the Covid pandemic, has also been associated with a growth with inequality
    - understand the relation between digital and inequality that of the digital divide: nations, regions, groups , individuals
    - A conceptual model is required to explain how digital inclusion may lead to inequality.

Labour exploitation: the gig economy (drivers, delivery workers) and platformisation of informal employment

The AI sweatshop (in India region) - Data labelers to train AI models. The ghost workers are well-educated workforce, many with STEM university education to an advanced level, but failed to find appropriate jobs in their actual field.

Commodification of data

India - biometric identification programme (Aadhar numbers). The approach is being exported to other regions including Sri Lanka.

The citizen became congruent with the customer, the national population is reborn as a “total Addressable Market”. January 2025 amendment to the Aadhar Act (2016) allows private sector services to be used to promote ease of living. Private innovation delivered through state-funded digital infrastructures empowers the poor and develops the nation. This allows predatory data profiling by the market which has never been enforced before.

- India’s DPI strategy of building health and agricultural data exchanges risks eroding the public value of the social data commons, due to the lack of attention to guardrails in data sharing partnerships.

Representational Injustice

- Stereotypical Word Association Test (SWAT) and Persona-based Scenarios Answering Task (PSAT) used to measure both implicit and explicit caste-based prejudices in LLMs. Continue to reflect entrenched caste stereotypes.

Concluding thoughts: Institutional governance deficits that perpetuate digital exclusion

- neocolonial digital order
- trade, tax and IP regimes entrench digital inequality - doesn’t able certain countries to create their own pathways
- Poverty of the imagination: South needs regenerative AI not more unicorns?

Notes from the discussion:

On Artificial Intelligence and AI transformation

How do you define AI transformation?

Referring to the UN Trade and Development's definition of AI, as the purpose of the technology, there is a transfer of structure in the economy. In AI, you see an introduction of technology service in the tertiary and private sector, in which there is an increased use of knowledge in its structure.

However, AI transformation doesn't mean it's magic as it does not necessarily leap through all the bottlenecks you have. If you are in the situation where you do not have any value added to the AI transformation, or giving up your data, then you would be lowered in the value chain.

With the proliferation of AI is not only the hype (and the illusion of 'inclusion" - everyone can now 'write', everyone now can 'draw'), but also the possible lack of solidarity that came with it - in AI labour displacement, first instinct is people might not protect one another, but to use the tools to replace our collaborators. We wish away designers, writers, we wish away project coordinators etc. Sure, AI lowers the barrier to working outside your lane, sure, that could mean more overlap between disciplines but individual work is often connected from the whole and when accelerated by automation, only makes the turbulence worse and the course corrections more violent

It is tantalising to see AI, such as the CoPilot revolution to make the work seen as dispensable. However, if we are increasingly seeing the internet as full of AI, chatbots and the transmission of information by way of AI becomes worse, there will be a point for collective response to stop using it. There is an increase in unionisation where people's jobs are affected by AI as well.

Q: Regarding copyright and content, is it the case of closing the barn door in case the horses have already left, especially when the data has already been stored and used by Big Tech, but the laws become better after?

I have never run into a situation where cognitive work can be extracted from the person, as the mind is not extractable. Generative AI is putting this to the test, but that's where there is hope to recognise this as work and not as similar to those fictions created by enterprises.

Another strategy is to reclaim copyright laws as content creators, and training standards.

In the case of data, one useful thing is that if we build data models, most businesses want access to continuously learn social relations. This requires continuous data collection, which requires a lot of work. This can be a way of 'rescuing the horse'.

There is also the debate on what kind of data could be commodified, and what shouldn't.We should recognise that data is social commerce, but model rights of traditional and indigenous knowledge should be acknowledged and involved. We should work on recognising the boundaries. Collective liaising on our data is a move we can prioritise.

Access to Connection and Data Control

In the previous session, we discussed the slow unionisation especially among gig workers. What pathways do you see to challenge through this divide?

- Due to the rapid development, what we're fighting is a sort of apathy. People see data as useless or as an inconvenience, and do not mind that their data is taken.
- The challenge is the concentration of wealth that one sees. It is timely that the digital rights group collaborates with the labour rights movement.
- Big Tech controls beyond the economy, as it also controls our agency, desire, and nature. To illustrate the danger of data mining, as it is not only colonising information but also on actual land sites for building data centres.
- Activists cannot stop only at surveillance and privacy, because even if privacy is granted by way of consensual data sharing, once the data is detached from the user, it will be reused for other means.
- Engage with each other in this group and submit proposals
- We also need a global ambassador to talk about the detriment of AI and lack of data privacy. We need a social communist response to this.

Even within this paradigm of the digital divide on who has access, there are varying degrees on what access and usage means. In SA, not many have the basic level of that connectivity. One may be connected but do not understand the complexities on how our data can be exploited. On the other hand, one may not be able to remain connected. We know that corporations' concern is on profitability. Could you please tell us more on the options of those alternatives? Such as responding with community work. You cannot prioritise one over another.

Even if people are not connected, the government has moved many systems online, especially in delivering their services, which could lead to life and death situations. E.g the hospital computer may not accurately recognise the patient's beneficiary or actual needs. We need to have the right to have a non-tech approach to many foundational services.

Secondly, we have abandoned the agenda of public access. In India, we do have a broadband fibre connection program. But it is not like a water pipe program - how do you make the connection meaningful? How do you make and deliver programs that can benefit many? 15 years ago, we were working on efforts to get connected. However, once mobile connection comes up, we tend to think of the mobile connection as a complete replacement for broadband internet, when these are two different infrastructures.

Because of the epidemic of misinformation, there is a rise in the debate for access, in which we can seize the opportunity to educate and talk about digital citizenship literacy and public access models. Many members of APCs are running this model, such as digital empowerment. We need to have a concerted response to lobby for a policy that can scale up these experiments.

Data and Labour Rights

Some 6-8 years ago IT for change had done a report that had looked at how datafication in ports in India such as Mumbai had tried port workers into amazon warehouse sequence stress bots. Their speed of movement was tracked with GPS, they had to complete tasks in some gamified but deeply punitive and unreasonable way. Amazon warehouse 101, really but in PPP port. To me this kind of example is a great way to show the horrors of data collection. However, I also see that the horror of this work model reflects equally perverse and inhumane work conditions in the informal economy.

This is a way to recognise the importance of Labour rights in countering this. Do you know of campaigns/organisation/initiatives dealing specifically with the labour conditions of datafication and gamified work?

In June 2025, ILO commits to International Standards on Gig Work which promises decent work in the platform economy. In India, because of unions like Indian Federation of App-based Transport Workers (IFAT) and All India Gig Workers Union (AIGWU), a range of parliaments have passed the legislations including one of them which looked at how algorithmic work management work systems are auditable by labour commissioners. These conversations on transparency and accountability on the trackers that we use are happening.

Even in the EU and in the UK, the unions have taken Uber under scrutiny. That's probably the way forward we can contest.

Certain apps and softwares also track how much time you spend on your devices, including keyboards and mouse. Sometimes software developers do not see themselves being affected by these issues. I wonder if we can create any solidarity through this?

Collective licensing of our data and workers data is something we need more investment in.

There is a popular movement on "why can't workers work with robots?" and we can comment on that.

Bossware - lots of civil society organising against this. I know that Business and Human Rights Resource Centre and Investor Alliance for Human Rights (not India specific though) has been doing a fair bit of work on this

Q: Some SA countries have passed or in the process of passing data protection laws, do any of them address the challenges on data protection and data rights? If not, what are the ways data protection legislation can address these problems?

If we look at the data protection frameworks emerging in the nation, the problem is it is trying to create a baseline by eliminating personal data to a publicly commodified market. This is not just true of our legislation, but also as the gold standard of EU-Data Privacy Framework (EU-DPF) which does not recognise anonymous data. The fact that if you have alienated data on the basis of free and informed concern, and aggregated on the anonymisation, the basis is that it can work as a Human Rights Free Zone.

The question of harm does not stop with the question of harm erosion. Downstream profiling and downstream capture of public value, the private sector has taken property. Unless you have means of compensatory purposes, how can you reclaim the public value of the data? This does not answer the question of benefit sharing outside of the legislation. What complicates this now is that, especially going by the experience of the African region, the pressure where India and Bangladesh have been negotiating with the US, digital trade becomes a bargain in which the US allows free reign on your market. That is one of the issues where we cannot imagine where we can see resources as data. We are only able to talk about personality data rights.

We are given the illusion to opt out from giving our data for the public and personal good. But there is also the question of having that option and choice to do so. In the concept of inclusion and access, as much as we want everyone to be included, does that include the option for people to meaningfully opt out?

I think if you look at European legislation, especially the Digital Services Act, there is an idea that users cannot lose the right to select services.

This is a fascinating way of thinking about GDPR. Do you have links to specific material on this for diving deeper into this perspective?

- https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4123311
- https://itforchange.net/index.php/treating-data-as-commons

Final Thoughts:

Suggests to read the Internet Feminist Report that APC created

- Feminist standpoint that FOE for all cannot stand without FOE for women and marginalised communities. What's the kind of free speech that we want on the internet? We do not want the liberal idea either, which could lead to amplifying certain speeches into power when we want to have an equal level.

Day 2 Report

Freedom of expression and privacy | 5:00 - 6:30 UTC

? **Prasanth Sugathan**

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:

Most state governments were initially not adept on regulating online media and platforms as opposed to physical media, due to the former being created and owned by private and independent sectors. With time, governments were able to exercise their control through legislative frameworks, partnerships, and monitoring. The impact is the online space, initially promised for independent ownership and free speech, has been filtered and with privacy compromised.

By looking and comparing the perspectives of various international and national human rights laws, there is an opportunity to challenge the legislation and the disparity on the private actors/platforms' treatment towards the Global South and the Global North. Participants can also learn from success stories of other countries.

International Human Rights Legislations

The session acknowledges that the right to Freedom of Expression (FoE) is a fundamental human right recognised internationally through these channels:

- Universal Declaration of Human Rights (UDHR): Article 19 guarantees everyone the right to freedom of expression
- International Covenant on Civil and Political Rights (ICCPR): Article 19 affirms the right to FoE, which includes the freedom to seek, receive and impart information and ideas “regardless of frontiers” and through “any other media of his choice”. This is not limited to offline/physical media, but also on online media.
- Online/Offline Parity: The Human Rights Council (HRC) has explicitly affirmed that the same rights that people have offline must also be protected online, especially freedom of expression.

National FoE Legislations and Restrictions in South Asia:

Constitutional/legal provisions generally ensure that an individual should have freedom of speech and expression. Different states have different levels of provisions on privacy, such as:

- Nepal has provisions to guarantee the right to privacy
- India recognises that privacy is a fundamental right

Fundamentally, FoE restrictions are meant to serve for the public good and reduce harmful behaviours, and must be proportionate and necessary, while serving legitimate aims (as per Article 19(3) of ICCPR). Unfortunately the definitions and implementations of the restrictions are disproportionate, with most often targeting voices of dissent such as journalists, individuals and whistleblowers reporting issues against any politically affiliated actors.

Such restriction categories are:

- Hate Speech - Should align with ICCPR Article 20, but most prosecuted under provisions like Section 153-A IPC, Now Section 196 BNS (India) or Anti-Terrorism Acts (Pakistan). Social media platforms are criticised for failing to enforce their own guidelines against actual hateful content made by politically affiliated actors. Enforcement is often inconsistent.
- Blasphemy/Religion - Mostly enforced against individuals and journalists, in protection of certain individuals rather than the idea of the religion itself. Examples are Bangladesh DSA Section 28, Pakistan PECA Section 37. Certain courts like Pakistani courts have encouraged aggressive state action, including blocking, against content insulting religion. Directly contradicts international calls for decriminalisation of blasphemy laws.
- Sedition/Political expression - Traditional penal codes are enforced online.
- Defamation - Vague definition on defamation content, and criminal defamation remains applicable. This is continuously discouraged by international human rights bodies who have asked for decriminalisation and imprisonment is not an appropriate penalty. Has a chilling effect on free speech.
- Contempt of Court - Used to clamp down on criticism of judicial processes and performance by journalists and lawyers. Violates ICCPR standards.

National Legislation in South Asia

Country	Constitutional/Legal Provisions	Key Permissible Restrictions (Non-Exhaustive)
India	Article 19(1)(a) guarantees FoE. Privacy is recognized as a fundamental right (*Puttaswamy I*).	Sovereignty, security of the State, public order, decency or morality, contempt of court, defamation, or incitement to an offence.
Pakistan	Article 19 guarantees FoE. Article 14 recognizes the privacy of the home.	Interest of the glory of Islam, integrity/security/defence of Pakistan, public order, decency or morality, contempt of court, commission of or incitement to an offence.
Bangladesh	Article 39 guarantees freedom of speech and expression	State security, friendly relations with foreign states, public order, decency or morality, contempt of court, defamation or incitement to an offence.
Nepal	Article 17(2)(a) guarantees FoE and opinion. Article 28 guarantees the right to privacy.	Acts undermining nationality/sovereignty, jeopardizing harmonious relations, inciting racial discrimination, defamation, contempt of court, or acts contrary to decent public behaviour or morality. (Article 17(3))
Sri Lanka	Guarantees freedom of speech and expression (Article 14(1)!a)).	Racial and religious harmony, parliamentary privilege, contempt of court, defamation, or incitement to an offence.

sflc.in

Restrictions on FoE in South Asia

Restriction Category	South Asian Legal Framework & Practice	Discrepancy with International Law
Hate Speech	Prosecuted under provisions like Section 153-A IPC - Now Section 196 BNS (India) or Anti-Terrorism Acts (Pakistan). Social media platforms are criticized for failing to enforce their own guidelines against hateful content, especially by politically affiliated actors.	Enforcement is often inconsistent, and platforms frequently allow speech that promotes hostility and violence to proliferate, contradicting international incitement standards.
Blasphemy/Religion	Retained and actively enforced, often extended to online spaces via ICT laws (e.g., Bangladesh DSA Section 28, Pakistan PECA Section 37). Pakistani courts have encouraged aggressive state action, including blocking, against content insulting religion.	Directly contradicts international calls for decriminalization of blasphemy laws.
Sedition/Political Expression	Traditional penal codes are extended online. While India's Supreme Court struck down Section 66A of the IT Act for its chilling effect and vagueness (*Shreya Singhal*), many overbroad laws persist, stifling dissent.	The vagueness of restrictions still allows for arbitrary criminalization of political criticism.
Defamation	Criminal defamation remains applicable (India, Nepal, Pakistan, Bangladesh). Courts have upheld its constitutional validity in India.	The continued use of criminal defamation is discouraged by human rights bodies.
Contempt of Court	Used to clamp down on criticism of judicial processes and performance by journalists and lawyers, creating a chilling effect (e.g., *In Re Prashant Bhushan*).	Violates ICCPR standards that contempt proceedings should only be used to maintain orderly proceedings, not stifle legitimate criticism.

Many social media platforms do not act accordingly in restricting harmful content, which often led to the state taking such actions online and even offline. Such issues and methods are:

- Content takedowns
- Platform accountability / content moderation
- Internet shutdowns - enforcing a disproportionate action that affects the larger public.

Such actions could cause a chilling effect of reducing free speech, instilling fear in expressing their opinions.

Three case studies in India: Safe harbour & intermediary protections

Safe harbour is mandated by Section 230 of the Communications Decency Act in the US.

Case 1, 2008, India: Avnish Bajaj vs State (Delhi High Court, 2008; SC, 2012).

Arrested as he landed in India for an obscene MMS sold via his own platform, baazee.com.

- Raised the question of the platform's liability for any content posted online, even if the platform owner was not the original poster.
- Section 79 of the Information Technology Act amended in 2008, but without any discussion in the parliament.

Case 2, 2011, India: Shreya Singhal v Union of India and connected cases.

In 2011, FB and social media pages were not widely used during this time as compared to now, thus the law was imposed on various individuals for vague reasons and activities such as for liking a post that is deemed unlawful, or tracking online ecommerce activities as alibi. Struck down Section 66A IT Act for criminalising "offensive" speech, ruled unconstitutional due to ambiguous wording and could lead to chilling effect on free speech.

- Although it is intended to protect marginalised/vulnerable communities, implementation showed otherwise as there was no clarity on the provision. There was a vague understanding on the terms and conditions, including on identifying content that is deemed as unlawful, and the order to take such content down within 36 hours. It also raises the question on the platform's accountability on considering unlawful content, or having the knowledge of doing so.
- Lawyers and CSOs reached out to the parliamentarians to look into the procedures, which prompted an MP to push a motion to annul these rules. This marked one of the rare cases where the subordinate rules and regulations on social media and online platforms were discussed and debated in the parliament. The media coverage of this debate further raised the public awareness on such issues.
- Clarified intermediary liability (Section 79 IT Act):
  - Intermediaries obliged to act on takedown requests only upon *court/government orders* citing limits of Article 19(2).
  - Overturned "notice-and-takedown by any person" regime, protecting platforms from adjudicating legality of all content
- Blocking rules found to be constitutionally valid, with the provision to hear the user's side.

Case 3, 2021: Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules.

These rules were tabled to regulate the proliferation of misinformation on WhatsApp, especially on tracking the source of forwarded messages. Other actions include proactive filters and a 24 hour takedown for illegal content.

This coincides with the Blocking Rules (2009), in which the government has the power to request the platform (WhatsApp or Facebook, and other platforms) to take down the unlawful content.

Although there is a provision to send notice to the affected party, this emergency provision is often used without any notice. The confidentiality provision also creates ambiguity in which the affected party will not receive the reasoning for the action.

In 2021, a FOSS engineer who maintains various FOSS domains and platforms, including Diaspora pod, Matrix instance Grounds filed a writ petition to challenge IT Rules 2021.

The terms used in Rule 3(1) are vague, making it uncertain on what is prohibited or permitted. Force the intermediaries to censor and restrict free speech, or lose “safe harbor” protection under the IT Act, 2000. It also impacts the right to privacy (Article 21), including the right to encryption, as it aims to introduce traceability and break end-to-end encryption.

Such rules can cause a disproportionate impact on small intermediaries or platforms, especially alternative or open source platforms run by small entities who may not have the capacity to fulfil such compliance and conduct thorough content tracing.

The writ petition is currently pending in Delhi High Court.

Blocking Instances

Mass blockings mostly occur during any protests or large dissent against politically affiliated actors or the state.

- India:
  - Geopolitical blockings such as TikTok and various Chinese apps
  - X handles and Youtube accounts during protests
  - Entire websites, such as The Wire, Tamil news website, being taken down due to one published content
  - Proton Mail - with the reasoning that there is low capacity of Indian nationality in its operations
  - OTT platforms - pornographic content
- Pakistan:
  - Youtube ban
- Nepal
  - Telegram

Other Legal Challenges in India

- The blocking of two apps, Briar & Element, versus UOI, were brought to court for the Intermediaries Rules 2021. Briar was accused of being used by terrorism in Kashmir, which became a reason for its blocking. Element is an open-sourced p2p network that is more secure than WhatsApp.
  - Intermediaries Rules 2021 - Challenges pending before the Delhi High Court
  - Blocking Rules - Confidentiality Provision - Supreme Court. The users do not get any information regarding the take down

    - Delhi High Court - Powers given to law enforcement to take down content, which finally revealed the details on the orders for the take down.
- Sahayog portal, where various agents can upload requests to take down certain content, was challenged by X at the Karnataka High Court. Unfortunately, the writ petition was dismissed with the appeal filed.
- High number of internet shutdowns in India: internetshutdowns.in

Grievance Appellate Committee (GAC)

Handles appeals from users dissatisfied with decisions made by Grievance Officers (GO) of social media and other online intermediaries. Users can reach out to GAC if they do not receive any response from the GOs, and can be challenged in court.
However, the GAC is not an independent body and is still largely governed and regulated by the state. There are no independent mechanisms and there is a huge lack of transparency in the structural and electoral processes. Some complaints are also filed once the platform responds with their defense.

Private actors and semi-private platforms' accountability

Users can use copyright infringement as a loophole and excuse for indiscriminate take downs to navigate any unlawful content. However, platforms most often do not follow the law or the jurisdiction. For Copyright, the DMCA provision requires notification and counter notification in which the rights holder needs to produce proof of cases. Cases that are filed in a defective manner with the affected user may never get a notice. Independent journalists and smaller content creators do not have the resources to fight such takedowns.

Platforms also do not assume nor take accountability on taking down the harmful content even after filing the report on hate speech or OGBV. The platform's own interest may go against the public good.

Organising and Mobilising on Platforms

Emerging digital spaces such as Discord, with gated servers, have become more central to grassroots mobilisation, like in Nepal, where online communities managed to drive political change through this platform. Youths were mostly moderating and mobilising, and is used as a communications channel to organise publicly.

However, such platforms have a double-edged sword on its lack of regulation and high number of users, as users are free to post any content in which some could be unlawful or incite violence against another user. The anonymity also doesn't promise absolute security, as there could be lurking surveillance from some actors or officers. The complexity of accessing Discord or platforms that are banned, which requires certain digital and technological literacy, means it's inaccessible to all communities and creates limitations in organising and mobilising. For example, only urban youths and digital literate people knew how to access Discord via VPN.

In Bangladesh, Facebook was being used for organising.

What is one provision in the law in your country that affects free speech in your country, that you would like to be amended or deleted?

India:

- Suggests to amend Section 292 of the Penal Code on obscenity in law, noting that it is meant to protect societal morality but often results in sexual-health educators and creators being wrongly flagged as “obscene.” The definition of obscenity is often being left vague, with legitimate educational content is often flagged while harmful misogynistic content is excused as free speech.
  - Suggests that the definition of obscenity should be modernised and made more inclusive, protecting free speech while still allowing appropriate regulation.
  - Notes that enforcement is a separate issue that also needs improvement.
  - Notes that Section 67A of the Information Technology IT Act, 2000, which punishes publications or transmissions of materials containing sexually explicit acts, is sufficient.
- Suggests abolishing Rule 31D of the IT Rules, which allows the government to issue immediate content-removal notices to intermediaries.
  - Points out conflict with the Shreya Singhal judgment, with Sahyog portal, which established stronger safeguards and a defined blocking mechanism through courts.
  - Emphasises that the current enforcement practices shape how “obscenity” takedowns occur, often without proper checks. The enforcement is placed on the intermediaries which often becomes compliant to the state
  - Section 66(A) through judiciary measures is sufficient. Points out that India already has a court-based blocking mechanism with review committees, safeguards missing in Rule 31D.
  - Warns that under state-level implementations, a single officer or telco authority may handle takedowns with no review mechanism, reducing accountability.

Bangladesh:

- Cybersecurity Ordinance Act, which allows authorities such as the Bangladesh Telecommunication Regulatory Commission (BTRC) to order content takedowns based on vague orders and broad grounds (claimed to work against national unity and economic threats.
  - Widely used by the previous regime, often without any judicial order.
  - Suggests to amend to require a judicial oversight.

Privacy, surveillance and data protection | 7:00 - 8:30 UTC

? **Ashwini Natesan**

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?

Definitions of Privacy

Participants' answered to what does privacy mean to them: Freedom from prying eyes; Control over my information; Unnoticed; Freedom; Being myself; Human rights; Civilised society; Non interference; Personal space; Protection

Historically, the right to privacy was first defined as the 'the right to be let alone' (Warren and Brandeis, 1890 Harvard Law article). For over a century, privacy law scholars labored to define the illusive concept of privacy.

The notion of 'control' acts as a common denominator, in which the definition of privacy is being reduced to: the control we have over information about and relating to ourselves.

- The second group highlighted 'access' as the essence of privacy, with a further subset called 'secrecy'.

A Taxonomy of Privacy, Solove (2006) - identified there are lots of rights that can be classified under the umbrella of privacy, with 16 harmful activities recognised under the rubric of privacy, and further classifying them into 4 groups. The field of privacy law has expanded to encompass a broad range of Information-based harms, including from consumer manipulation to algorithmic bias.

Privacy by essence goes beyond data, as it affects the physical life. Every person should have autonomy on the information on their body, identity and physical space. For this discussion and based on the statutes and legislations available, privacy is narrowly defined under the banner of data protection.

Four Stages of Information and Data Management

‘Data Subject’ is an individual whose data is being subjected/collected. There are four stages of processes that could happen to the data:

- Information collection - What is the data being collected? Information that’s being collected to define you as an individual.
  - Surveillance - intrusive
  - interrogation
- Information processing- how is the information being used?
  - Segregation
  - Identification
  - Insecurity
  - Secondary use
  - exclusion
- Information dissemination - where does the information get shared/dissemination? In most cases, some of the data are being shared without the knowledge of the data subject
  - Breach of confidentiality
  - Disclosure
  - Exposure
  - Increased accessibility
  - Blackmail
  - Appropriation
  - distortion
- Invasions
  - Intrusion
  - Decisional interference - how we have autonomy to define the dissemination

Privacy Rights in the Digital Age

Privacy rights in the digital age are commonly understood as the right and expectation of individuals to control the collection, use, and sharing of their personal information (data, communications, conduct) in the digital realm. Not just secrecy, but autonomy and control over one’s digital self.

- Key components:
  - Information privacy: protection of personal data collected and stored by entities
  - Communication privacy: protection against unauthorised interception or access to personal communications (e.g. emails, messages)
  - Individual privacy/identity: safeguarding one’s digital identity and online persona

Privacy is often thought of as an individual interest, and does not breach into the public good. In this sense, privacy is often pitted against other rights and freedoms more broadly “social values” such as free speech, security, innovation, efficiency and transparency.

This view is narrow and does not capture privacy as a social value - in at least two ways:

- Protects individuals for the sake of the greater social good. This leads into surveillance, in which the safeguards and transparency on its functions needed to be discussed more.
- Construct societal frameworks that distribute power more fairly and productively. Power is often associated with state and government, but current markets show that private actors and sectors are also accountable.

The right to privacy aims to preserve human dignity and autonomy, as the latter is and should be non-negotiable. The right to make decisions is currently being influenced by parties who do not have our best interests in mind.

- Prevents misuse and harm
  - Identity theft and financial fraud
  - Manipulation (eg through targeted disinformation)
  - Cybercrime and online harassment

Contextual Understanding of Privacy

In the South Asia context, there is a lack of actual Data Protection Laws unlike in the Global North. Legislatively and culturally, privacy is not seen as a priority in most legislations, and sometimes ranked lower than other general rights. It has assumed a secondary role compared to other issues such as national security.

As noted by Anuvind, it is often framed antithetical to certain positive actions, especially crime prevention, as if "nothing to hide means nothing to fear" - but rather than centering this discourse around the "misuse" of the right to privacy, it is often discussed as a reason to not have such a 'right to privacy' in the first place.

However, the debate itself is wrong because it is mostly framed from the POV of someone else needing access to that information, rather than on the need and right for an individual to protect their own data. There is also no clarity on why other issues should be prioritised, when there is intersectionality in all cases.

Current Legal Frameworks

- Sri Lanka: Modelled after EU GDPR. Focused on how the data is being processed and transferred. An individual has the right of information, in which they also have the power to deny information requests if the request does not align with your interest.
- India: Digital Personal Data Protection Act (DPDP) 2023, DPDP Rules 2025: defined a class called Significant Data Fiduciaries (SDFs) as the controller, who must follow stricter rules (e.g. appoint a Data Protection Officer). Individuals (‘data principles’) are granted rights such as access, correction and erasure of their data. There are heavy penalties for non-compliance
  - DPDP Rules - Phased implementation
  - Eg: The SDF/Controller is an individual who is in charge of managing a personal database of the company’s frequent customers. The concern is when additional storage is required, the Controller would resort to using external services such as

Cloud systems offered by other providers. The Cloud system would have their own processing of the data.

- Bangladesh: Personal Data Protection Ordinance (PDPO): personal data refers to any information that can identify an individual - including names, addresses, financial information, location, health details, biometric data, and other information.
- Pakistan: no law in place when it comes to Data Protection, currently being drafted. Currently there is some pushback from the US on Pakistan's draft that is following the EU's GDPR framework.
- Nepal: Individual Privacy Act 2018 ("Act") // Individual Privacy Regulation, 2020. Strives to protect the fundamental

Legal Challenges:

- Enforcement mechanism, which should ideally be an independent regulatory body with clear appointment processes.
- Broad exemptions for government agencies
- Low public awareness and digital literacy due to the culture's conversation on privacy in general
- Existing laws do not sufficiently address risks like algorithmic bias and the need for transparency in automated decision-making. Many decisions are now automated with no human check-and-balance.
  - Traditionally, GDPR is where protections are given for automated decision-making. For instance, a loan application being processed by an automated system that decides on the approval based on preset requirements without any additional nuances
- Data protection frameworks often contain large, sweeping exemptions for "national security" or "public interest"

Consent

'Consent' is rarely informed. Most laws have a provision that personal data can be collected, provided the individual consent to the processing of the data. But there is no real choice afforded in our terms and conditions (T&C), Thus the flaw is that consent is assumed to be a catch all process.

Behavioral experiences noted that many users do not have time to go through the T&C, and in some cases, do not have a choice in accepting the T&C if there is a strong need to use the services.

The recent example of most platforms' terms of service that automatically entails all user content will be used to train for LLM and it is difficult to opt out, and scraped data made without consent. This further pools into the extent to how much entities, corps, individuals, groups are allowed to have access to users. Some suggestions on user-empowering consent mechanisms should look like:

- Option 1: to have a visible option to opt out from those services (when ideally there should also be a choice to opt in). If such a choice is not made available, consent is meaningless and the PDPR Act should interfere. An alternative is for the user to resist from providing any meaningful content (does not want the content to be shared for this purpose).
- Option 2: If individuals need to navigate the providers, a third party should interfere.
- Option 3: Consent should be renewed from time-to-time. Either by every update or every few years.

Surveillance by private actors and companies

Big Tech companies thrive on users' data, evidently through targeted ads that are based on data collection and profiling. Companies collect vast amounts of user data via their digital footprint, which could be but not limited to:

  - Social media: users own updates, engagements, networks and connections
  - Apps and websites: browsing history, purchase patterns, cookies and trackers
  - Smart devices (IoT): data on daily routines from smart speakers, fitness trackers, and connected cars

These data are further integrated into the surveillance mechanism, where it is used to create detailed profiles for targeted advertising and market manipulation, often without the user's full comprehension or meaningful consent ("consent fatigue").

Surveillance capitalism by Harvard economist Shoshana Zuboff explains it as:

- Incursion - the user enters an area of data collection
- Habituation - the user gains a habit and does not consider the repercussions
- Adaption/Adaptation - the user agrees to the narrative
- Redirection - the user is forced to focus on the little aspects being considered without looking at it holistically

The relationship between State and Private Actors

- Surveillance capitalism is often being seen in insurance and government surveillance markets partnerships.
- Aadhar Authentication for Good Governance (Social Welfare, Innovation, Knowledge) Amendment Rules, 2025.
- Need to use data for the public good, but to be more transparent with the systems in place, ensuring that they protect and preserve rights.
- Consent, particularly, on the reliance of another entity
- India can set the standard for ethical Digital ID governance.

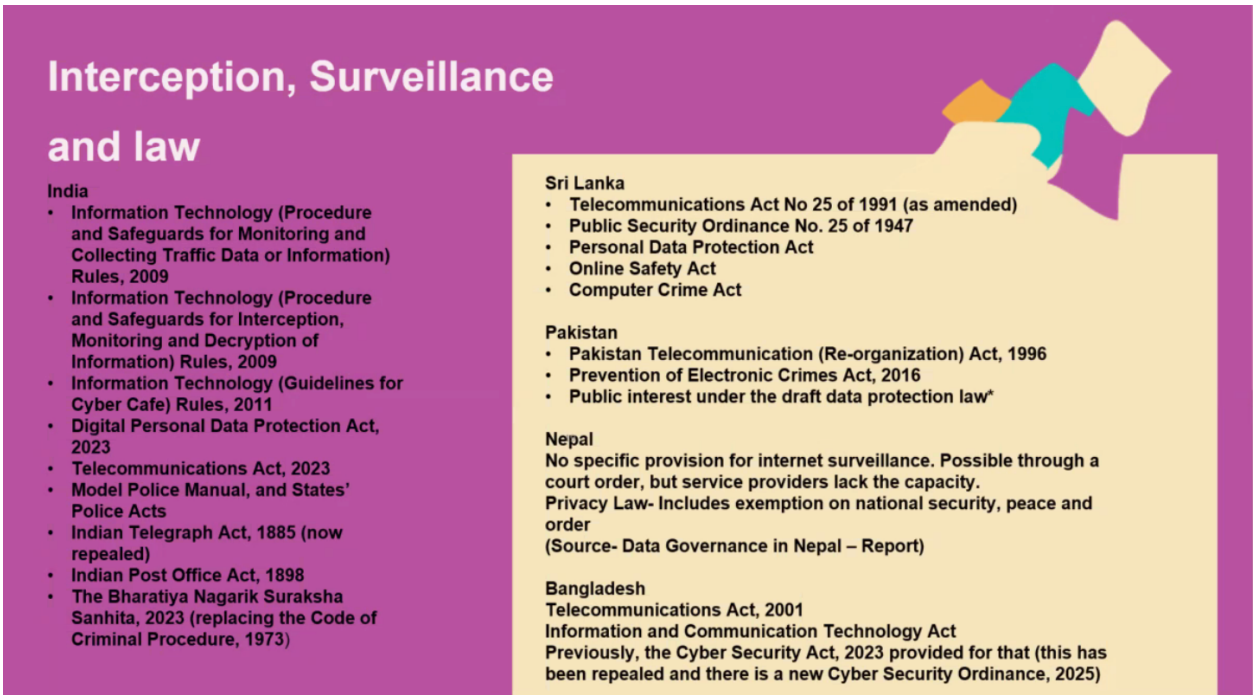
State Surveillance and Control

- Mass surveillance through telecom metadata collection
- Interception of communication (telecommunication)
- Social media monitoring for dissent

- Use of spyware (Recall Pegasus) and device hacking tools
- Biometric national ID systems linked to services

Case: India - Fundamental right - Justice K.S Puttaswamy (Retd) & Anr vs Union of India

- Privacy is deemed as a social construct. These observations from the Supreme Court in India pronounced privacy to be a distinct right under Article 21 of the Constitution - one that covered the body and mind, including decisions, choices, information and freedom
- Specifically mentioning that it also focused on various safeguards that should be kept in case of national identities, rejects that privacy of an individual is an elitist construct.



Impact on Freedoms (Expression, Assembly, Association)

Chilling effect on FoE:

- Suppression of Assembly and Association
  - Used to identify organisers and participants of peaceful protests
  - Monitor private communications related to political organising or trade union activities, thereby chilling the right to association
  - In extreme cases, arbitrary detention or legal action under vaguely worded security laws
- Targeting and discrimination
  - Human rights defenders or journalists
  - Ethnic and religious minorities
  - Women and LGBTQ+ communities
- Digital exclusion:
  - Lack of safeguards, especially in the context of digital ID systems, can be used as a tool of exclusion, denying access to public services or provisions for those who cannot or will not provide extensive personal data

Can there be lawful and justified surveillance?

In the opinion of yes, there needs to be surveillance that has to go through the principles of:

- Legality - accordance with a law
- Legitimate aim that does not require an extremely invasive measure
- Suitability - adequacy
- Necessity (least restrictive measure) & proportionality stricto sensu - the harm caused to the individual by the restriction must not be excessive in relation to the benefit gained by achieving the public interest aim
- Procedural safeguards which should entails having an independent regulatory committee, that determines any rules or regulations before conducting the surveillance

Private actors can be held accountable by having a strong data protection law in place, followed by strong law enforcement and implementations. Since 2018, the instances of EU GDPR enforcement particularly against BigTech has been very encouraging in showing that an individual's access to their rights can be achieved through judiciary and other mechanisms.

Concluding Thoughts

Privacy is essential for autonomy and democratic rights. With the spread of biometric ID systems, SA faces growing concerns over surveillance. This can be mitigated by strong independent oversight, governed by a strong Data Protection Act.

Civil society should also play a bigger role in safeguarding the rights.

As an individual, one need to constantly ask:

- How is the data being shared?
- What is it being shared for?
- Where is it being shared?
- What are the protection mechanisms?

Reflection questions:

- Privacy as a right is not only about protection personal data (but, we are limited to this because of the statutes and laws we currently have)
- Surveillance is not limited to the State but also to private actors
- What are some of the use cases in your State for surveillance?
- Are the measures justified under the human rights test of legality and proportionality?

Group Discussion - privacy and surveillance: Group 3 - Case Study on Privacy and Surveillance_South Asia

- The current laws give the government too much power on what they can do, rather than on what they cannot or should not do.
- The government will push against the universities if they do not comply

Day 3 Report

(To be updated)