MODULE 3:
ACCESS TO THE INTERNET

K.S. Park
kyungsinpark@korea.ac.kr
Korea University Law School, Open Net

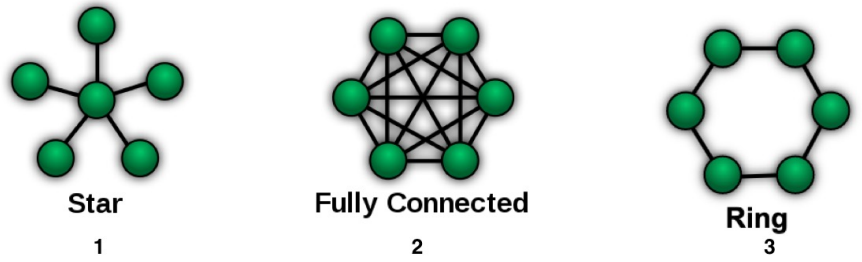
Litigating Digital Rights and Freedom of Expression Online

Overview

- An obligation on States to progressively promote access to the internet is emerging under international law, in recognition of the fact that access to the internet enables freedom of expression and a variety of other fundamental rights.
- Practices such as internet shutdowns and blocking and filtering of content are severe restrictions on the right to freedom of expression which often do not constitute justifiable limitations.
- 'Net neutrality' refers to the principle that all internet data should be treated equally without discrimination based on the device, content, author, origin and/or destination of the content, service or application.
- Intermediary liability occurs where technological intermediaries, such as internet service providers (ISPs) and websites, may be held legally liable for unlawful or harmful content created by users of those services. Such liability has a chilling effect on freedom of expression online.
- Administrative censorship occurs when contents are taken down by administrative bodies.
- Anonymity restrictions take place when digital speakers are required to identify themselves so that they can be tracked down by authorities for their online speech.

Nature of Internet

- Extremely distributed communication system – “There is no center in the internet.”
- Which one is freer?



- Role of routers and routing tables.
- Any-to-any communication what if crowded by big mouths?
- Web vs email – Client-server mode of communication – request for contents answered by server – 100% consensual communication
- Internet gives every individual the power of mass communication → democracy, economic development, and information revolution!
- “Internet allows weaker (by age, social status, gender, wealth, etc.) groups to speak on equal footing” (2012, Korean Const Crt on real name)

Access to the Internet

- No human rights treaty explicitly recognises a right to access the internet because they were developed before the internet became popular.
- However, due to its key role in facilitating freedom of expression, a growing body of authoritative statements indicate that states must take progressive steps to ensure universal access to the internet. (2012, 2014, 2016, 2018 Human Rights Council Resolution: "What is protected offline should be protected online")
- A lack of access to the internet can exacerbate existing socio-economic divisions.
  - For example, a lack of access to the internet can impede an individual's ability to obtain key information, facilitate trade, search for jobs, or consume goods and services.

The UN Sustainable Development Goals (SDGs)

- The SDGs recognise the importance of communications technologies to sustainable development. Examples:
  - **Goal 5(b)**: Enhance the use of enabling technology, in particular information and communications technology, to promote the empowerment of women.
  - **Goal 9(c)**: Significantly increase access to information and communications technology and strive to provide universal and affordable access to the Internet in least developed countries by 2020.
- The 2016 UN Human Rights Council Resolution on the Internet also recognises that the internet can accelerate progress towards development and affirms the importance of a rights-based approach to providing internet access.

The Right to Internet under International Law

- It is increasingly being recognised that the internet is now central to the exercise of freedom of expression and numerous other fundamental rights.
  - In 2003, UNESCO was among the first international bodies to call on states to take steps to realise a right of access to the internet.
  - In successive Joint Declarations, the special international mandates on freedom of expression at the UN, OSCE, OAS and African Commission have made it clear that they view the right to freedom of expression as including an obligation on states to promote universal access to the internet
  - In *Kalda v Estonia* (2016), the European Court of Human Rights held that the applicant's right to freedom of expression had been violated through a prison's refusal to grant him access to internet websites containing legal information.
  - Several countries (for example, Greece, Estonia, Finland, Spain, Costa Rica and France) have recognised some legal right of access to the internet.

Access to Internet as a Human Right

- The human right to access the internet is “with a view to achieving the full realization” over time, rather than immediately, similar to social and economic rights, such as the right to education.
- The internet is different than other technologies (for example, broadcasting or print media), because it is so significant to daily life, especially as an expressive medium.
- The internet is increasing recognized as indispensable to the enjoyment of fundamental rights:
  - A lack of access exacerbates existing socio-economic inequality.
  - A lack of access impedes an individual’s ability to obtain key information, facilitate trade, search for jobs, or consume goods and services.
- Access entails the technological ability to make use of the internet in a manner that is affordable, safe, secure, effective and meaningful.

Interferences with Access to Internet

Examples: Internet shutdowns, disruption of online networks and social media sites, blocking and filtering of content

- Disrupting or blocking access to internet services is a form of prior restraint, i.e. prohibiting speech or other forms of expression before they can take place.
  - The International Covenant on Civil and Political Rights prohibits most forms of prior restraint because of the extreme chilling effect on freedom of expression.
  - The American Convention on Human Rights contains a more explicit prohibition on prior restraint.
- For a restriction to be permissible, it must meet the three-part limitations test set out in article 19 of the ICCPR, which requires it to be:
  1. Provided by law
  2. For legitimate purposes (respect for rights/reputations of others; protection of national security, public order, public health or morals)
  3. Necessary

Internet Shutdowns

- **Definition:** An intentional disruption of internet or mobile communications rendering them inaccessible or effectively unusable for a specific population or within a location, often to exert control over the flow of information.
- Shutdowns range from a total network outage—where access is blocked entirely—to where access is throttled or rendered effectively unusable, whether to the whole internet or mobile communications, or just some websites.
- Shutdowns may affect an entire country, regions within a country or even multiple countries, and may range from several hours to several months
- In order to conduct shutdowns, governments typically require the collaboration of private actors which operate networks or facilitate network traffic.
- Large-scale attacks on network infrastructure committed by private parties, such as distributed denial-of-service (known as 'DDoS') attacks, may also have shutdown effects.

Internet Shutdowns in Myanmar

- Internet shutdowns have been common in Myanmar for some time.
- Since the February 2021 *coup d'état* in Myanmar, the military regime has repeatedly resorted to internet shutdowns, although they were also in place before that.
- The shutdowns have taken different forms, such as national or regional blackouts, and impeding access through speed restrictions and increased data fees.
- Myanmar is not the only example; in 2021, internet shutdowns were also documented in India, Bangladesh, Indonesia and Pakistan.

Blocking and Filtering of Content

- "**Filtering** is commonly associated with the use of technology that blocks pages by reference to certain characteristics, such as traffic patterns, protocols or keywords, or on the basis of their perceived connection to content deemed inappropriate or unlawful;
- **Blocking**, by contrast, usually refers to preventing access to specific websites, domains, IP addresses, protocols or services included on a blacklist."

The 2011 Joint Declaration on Freedom of Expression and the Internet

a) Mandatory blocking of entire websites, IP [internet protocol] addresses, ports, network protocols or types of uses (such as social networking) is an extreme measure – analogous to banning a newspaper or broadcaster – which can only be justified in accordance with international standards, for example where necessary to protect children against sexual abuse.

b) Content filtering systems which are imposed by a government or commercial service provider and which are not end-user controlled are a form of prior censorship and are not justifiable as a restriction on freedom of expression.

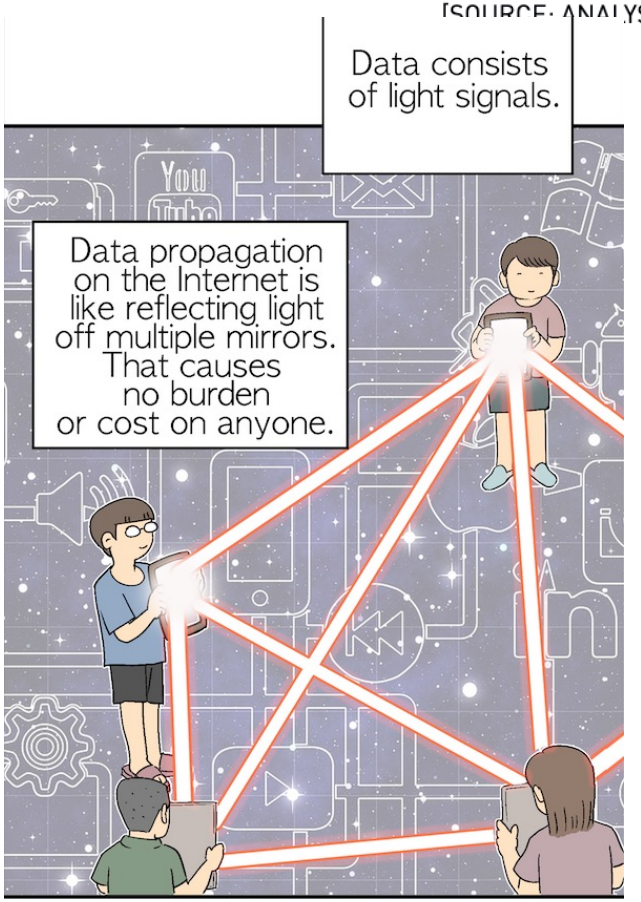
c) Products designed to facilitate end-user filtering should be required to be accompanied by clear information to end-users about how they work and their potential pitfalls in terms of over-inclusive filtering.

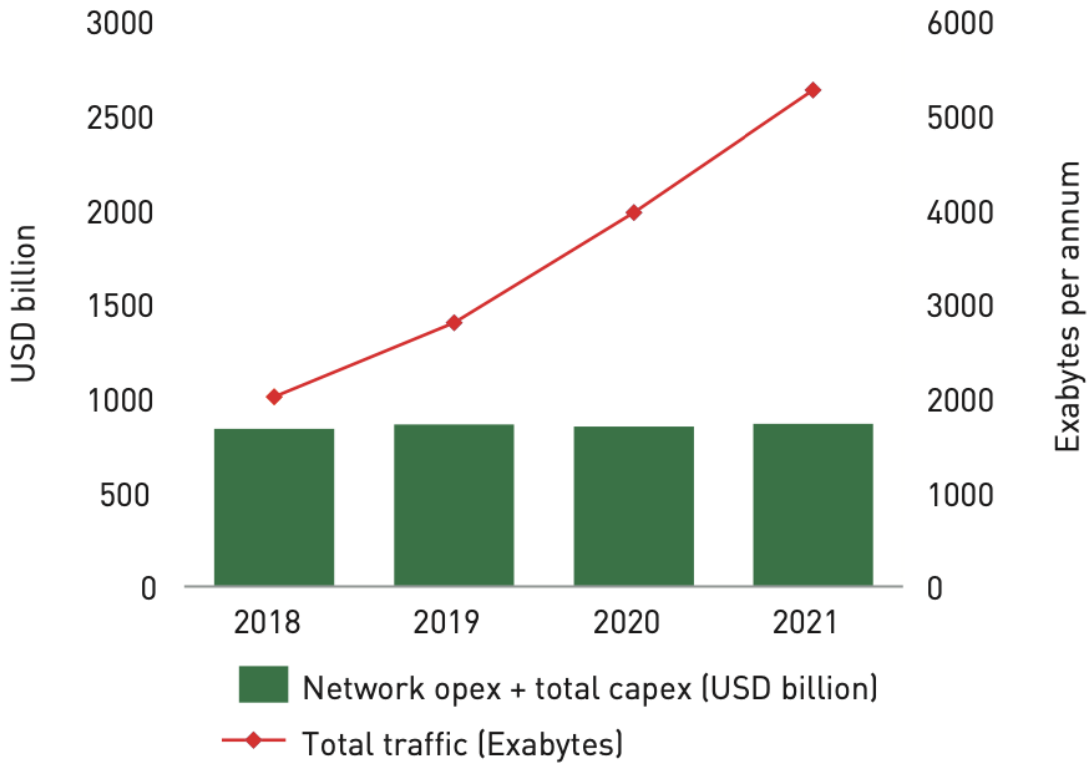
Network Neutrality ('Net Neutrality')

- **Definition:** the principle that there should be no discrimination in the treatment of Internet data and traffic, based on the device, content, author, origin and/or destination of the content, service, application, or payment.
- Discrimination may involve halting, slowing or otherwise tampering with the transfer of any data, except for a legitimate network management purpose, such as easing congestion or blocking spam.
- Why? Nature of internet. **Information revolution is impossible without net neutrality.**
- Two key ways net neutrality may be undermined (2017 Report of the UNSR on freedom of expression):
  - **Paid prioritisation ("network usage fee") schemes:** giving preferential treatment to certain types of internet traffic for payment or other commercial benefit.
  - **Zero-rating:** not charging for use of internet data associated with a particular application or service while other services are subject to metered cost.

FIGURE 0.2: GROWTH IN TRAFFIC DELIVERED OVER FIXED AND MOBILE ACCESS NETWORKS, AND EVOLUTION OF NETWORK-RELATED TELECOM OPERATOR COSTS FROM 2018 TO 2021

[SOURCE: ANALYSYS MASON RESEARCH, ANALYSYS MASON, 2022]





Zero-Rating in Asia

- There has been significant debate in various countries in Asia about access to zero-rated content.
- Social networking sites often offer zero-rating schemes.
- They argue that zero-rating provides access to people who might not otherwise have been able to access the internet.
- But, in practice, users often get stuck just accessing the privileged services and may even think that these comprise the whole internet.
- India is among the jurisdictions that has taken action again zero-rating, effectively banning it.

Limitations to Freedom of Expression

Internet Shutdowns

- Under international human rights law, internet shutdowns are always unjustifiable restrictions of freedom of expression due to being excessive.

Blocking and filtering

- Blocking and filtering of content may be justifiable in certain circumstances (for example, websites distributing child pornography) if they meet the three-part test for a justifiable restriction, as assessed on a case-by-case basis.

Net Neutrality

- Limitations to network neutrality may be permissible in certain circumstances (for example, legitimate network management purposes).
- But, this is exceptional and internet intermediaries should be transparent about any traffic or information management practices they employ.

Bhasin v. Union of India (2020)

- The Supreme Court of India considered the legality of an internet shutdown in Kashmir.
- The Court found that a complete shutdown of the internet was a 'drastic measure' that should be "considered by the State only if 'necessary' and 'unavoidable.'"
- The State "must assess the existence of an alternate less intrusive remedy" and any shutdown of the internet must meet the requirement of proportionality and not extend longer than necessary.
- International standards go even farther. Under international human rights law, internet shutdowns are always unjustifiable restrictions of freedom of expression.

National Security as a Justification

- National security is frequently relied upon as justification for an interference with access to the internet and other restrictions on freedom of expression.
- National security is one of the legitimate grounds for restricting freedom of expression online in certain circumstances but it is also often abused to quell dissent and cover up state abuses.
- Where freedom of expression online is restricted, there should be transparency regarding the laws, policies and practices relied upon, clear definitions of terms such as ‘national security’ and ‘terrorism’, and independent and impartial oversight of measures.

Intermediary Liability

Intermediary liability: where online intermediaries, such as internet service providers (ISPs) and websites, can be held legally liable for unlawful content disseminated by users of those services (for example, copyright infringements, digital piracy, defamation and hate speech).

- The importance of limiting the liability of intermediaries:
  - Essential to the flourishing of internet services that facilitate expression
  - Intermediary liability is often incompatible with human rights norms
  - Unlike due process required of law enforcement, governments are frequently opaque about requests to companies to restrict content and other surveillance measures.
- Intermediaries can serve as an important defence against government and private overreach, such as pushing back on a shutdown. This is only possible without fear of sanction or penalties (2017 report by UNSR on freedom of expression).

Protection of Intermediaries

- Systems of protection for intermediaries:
  1. Absolute immunity from liability
  2. Liability only following refusal to obey an order from a court or other competent body to remove the impugned content
- The 2011 Joint Declaration:
  - Intermediaries should be liable only for third party content when they specifically intervene in that content or refuse to obey an order to remove it adopted in accordance with due process guarantees.

Case Law on Intermediary Liability

The European Court of Human Rights

- *MTE v Hungary (2016):* The domestic courts were not justified in assigning intermediary liability for comments that were offensive and vulgar, but not unlawful.
- *Tamiz v UK (2017):* ISPs should not be obliged to monitor content or proactively investigate potential defamatory activity on their sites.
- *Delfi AS v Estonia (2013):* The domestic courts were justified in finding that an internet news portal was liable for illegal comments posted by readers.

Supreme Court of India

- *Shreya Singhal v Union of India (2012):* Liability exists only where an intermediary has received a court order or has been notified by government of an unlawful act and has failed to act.

Supreme Court of Argentina

- *María Belén Rodriguez v Google (2014):* Search engines are under no duty to monitor the legality of third-party content to which they link and can only be made to remove content where there is "gross and manifest harm."

Administrative censorship

1. Bias in decision making compared to judiciary:
   →Criticisms of incumbents more likely to be taken down
2. ”provisional” before court decision → “chilling effects”

- “Administrative bodies always act first!”

e.g., FDA banning certain food items

→But ”chilling effect” problem applicable only for speech

International comparison on administrative censorship

- No administrative censorship on internet generally
- Only broadcasting: state grant of monopoly
- Pre-2017 Internet administrative censorship- only in China, Korea, Turkey, Australia (only in child porno)
- Banned as unconstitutional in Spain (2022 Women on Web), France (2020 Avia hate speech law, 2009 3-strike-out copyright law), Philippines (2014 Cybercrime Prevent Act), and USA (Bantam Books v Sullivan)
- But rising in Southeast Asia: Thailand, Indonesia, Vietnam, Singapore, and Myanmar
- Vagueness of standard rampant: “prohibited content”, “against the state”, etc.

Approach to RTBF - Data protection law

- "Data surveillance" – Surveillance done with data turned over consensually – use for other purposes – transfer to 3rd parties
- Unequal bargaining power → Solution: **ownership** instead of contractual control
- Data controllers' obligation = Data subjects' rights
- Obligation not to **process** unless **consent** or 5 other legal bases (including **public interest**)
- Data subjects' direct rights
  - right to **access** and **correction**
  - right **to erasure** and **stop processing (right to be forgotten – Does publicly available data require ownership-based intervention?)**

Conclusion

- The right of access to the internet is increasingly recognised as an indispensable enabler of the right to freedom of expression.
- Restrictions on access to the internet unduly infringe on freedom of expression and associated rights unless they conform to the three-part test for such restrictions.
- Proper standards relating to issues such as internet shutdowns, blocking and filtering of content, net neutrality, intermediary liability, and administrative censorship are necessary to fully protect and promote the right to freedom of expression online.