Human rights based proposals for model laws on Internet shutdowns and platform blockings

K.S. Park, kyungsinpark@korea.ac.kr

Open Net, Korea University, FOC, GNI

High Level Panel on Global Medial Freedom Initiative

Standard model

- Access Now (2016, Primer): “ICCPR 3-part test sufficient. Just need guidance. No single internet shutdown meets the test”
  - Legality - Legtimate aim – Necessary and Proportionate
- 2011 UN HRCee’s GC 34, para 34 – “must be content-specific”, “generic bans not allowed on certain sites and systems”
- UNHRC “online=offline” (2012, 4, 6, 8) – what does it mean? Existence of online ”as a precondition”? Not helpful. Maybe interpretable in reference to water-tight prior censorship
- 2016 UNHRC “should not prevent or disrupt access to info dissemsination in violation of int’l law”
- UN & regional FOX Special Rapporteurs – mainly condemning from N/P angle and protecting access to knowledge

→ Maybe clear on internet shutdowns, NOT specific enough to provide litigational support or abate platform blockings with granular normativity

Difficulty – so many laws cf. stopping shutdowns

- 2019 UK shutdown London underground to stop climate protests
- 2011 SF shutdown of mobile internet in subway to control a protest
- GNI 53 countries survey + Freedom on Net (2017-8) 66 countries survey → 47/55 laws enabling shutdowns and 52/57 blockings

Shutdown laws (55 countries)

- 21 countries[90] have “license condition”, “regulatory violation” as the most frequent bases for shutdowns.
- 18 countries list “national security”, “public safety”, “national integrity”, “civil protection”, “public order”, “public interest” or similarly vague reasons as the second most frequent bases for shutdowns.
- 9 countries list “war”, “emergency”, “terrorism”, “injury” and similarly narrow reasons as the third most frequent bases for shutdowns, while not allowing broader bases for shutdown such as “national security”, “public safety”, etc.
- 8 countries list “crimes”, “illegal activities”, “administration of justice”, “refusal to block illegal information” and similar reasons as the bases for shutdowns
- 8 countries have no bases for shutdowns.
- Only Montenegro and El Salvardo require judicial approval for all shutdowns while Kazakhstan and Jordan require court approval for part of the shutdowns.
- Only South Africa and Germany permit an internal appeal by ISPs against shutdown orders, while most countries allow ordinary administrative lawsuits or constitutional challenges against shutdowns mostly after they are instituted.

Blocking laws (57 countries)

- 26 countries have “crimes’, “violation of law”, and “illicit/ illegal content”, and “illegal activities” as the most frequent bases of website blocking.
- 15 countries list “national security”, “national integrity”, “national sovereignty”, “public order”, “public interest” as the second most frequent bases of website blocking.
- 12 countries list “war”, “emergency”, “terrorism”, “injury”, “defense’, and other physical harms as the third frequently cited basis of website blocking.
- Uniquely for website blocking, 5 countries list “anti-government”, “violation of dignity of monarchy”, “seditious publication”, and “image of the state” as the basis of website blocking”.
- There are other less frequently appearing bases for website blocking such as intellectual property rights, child protection, pornography, and hate speech.
- As expected, there are more court-based procedures (7 countries) for website blockings than shutdowns (2 countries).
- As to administratively enforced actions, internal appellate procedure is still far between for website blocking as for shutdowns (only Germany).

Challenges of drafting a “Model (soft international) Law” on Internet shutdowns

- Definitional: internet shutdown vs platform blockings
  - What are we fighting for? PB can be damaging as IS but PB bleeds into blocking-type content moderation which we cannot completely ban
- Legal: ITU Constitution Ch. IV-4, Article 34(2) – States reserve the right to cut off private telecommunications dangerous to national security
- Structural: ISPs receiving grant of public goods – bandwidth and easement on underground conduits and electric poles → “public interest obligations” → who decides what is in public interest → open up legal room for govt to engage in internet shutdown

2nd-order Objectives

- How to support litigations against internet shutdowns – procedural and statutory roadblocks more effective than substantive (Rathi & Basu, ”Dialing in the Law”, APC, 2020)
- How to support ISPs in challenging shutdown orders –appeals to internet shutdown order – ex post/ante judicial orders
- Granular legislations that support necessity and proportionality - prevent “hammer-nail” thinking
  - Web pages (URL) v. web sites (TLD)
  - Content v. URL/TLD
  - Blocking v. Takedown
  - ISP v. CP
  - General purpose platform v. Special purpose platform
- ISP’s public interest obligations enforced through shutdown v. fines

Recommendations for model law

- Shutdown & general purpose platform blocking – not allowed at all times even regionally unless consented to by users (no more subway WIFI shutdown)
- Special purpose platform blocking (Akdeniz) & non-platform blocking (& takedown)– judicially ordered – Manilar Principles for Intermediary Liability → if urgent, administrative appeal (Germany)
- Judicial standard must N/P and must include 'prior censorship' analysis (Inter-American Com HR)and 'retaliatory ban' analysis (Brazil *Whatsapp* ban)
- ISPs disciplined only civilly, should not involve shutdown of service → if license taken away, public "taking"

Big question

- **Will a model law invite more internet shutdowns?**

- Gregorio & Stremlau, “Internet Shutdowns and the Limits of Law” International Journal of Communication 14(2020), 4224–4243
- Tomiwa Ilori, “Life Interrupted”, GNI (2020)