IGF 2022
Policy Network on Internet Fragmentation
(PNIF)

PNIF session at the 17th IGF annual meeting   30 November 2022
Addis Ababa, Ethiopia

Meeting agenda
1. *Welcome*
2. *The Policy Network on Internet Fragmentation (PNIF) - introduction*
3. *Towards a framework for discussing internet fragmentation*
   3.1. *Unpacking the framework*
   3.2. *Town hall discussion on internet fragmentation and the draft framework*
   3.3. *Summary of the discussion and input for the Main Session*
4. *Looking forward - next steps for the PNIF*

Discussants
Ms Mazuba Haanyama, *Head of Human rights Policy, Africa Middle East & Turkey, Meta;* **Ms Nawal Omar,** *Researcher at ICT Africa;* Mr Olaf Kolkman, *Principal at Internet Society;* **Mr Túlio César Mourthé de Alvim Andrade**, *Deputy Head, Brazilian Ministry of Foreign Affairs.*

Moderation & Coordination
Ms Sheetal Kumar, *PNIF co-coordinator,* **Ms Bruna Martins dos Santos**, *PNIF co-coordinator,* **Mr Wim Degezelle**, *IGF consultant PNIF.*

Session transcript and recording
https://www.intgovforum.org/en/content/igf-2022-day-2-pn-internet-fragmentation

Meeting Summary

PNIF Introduction.

The Policy Network on Internet Fragmentation (PNIF) is an IGF intersessional activity to further the discussion on and to raise awareness of the technical, policy, legal and regulatory measures and actions that pose a risk to the open, interconnected and interoperable Internet.

The PNIF proposal is born from a multistakeholder community initiative and the objectives of the PNIF - over an envisaged 2 year timeframe - are to (a) Offer a systematic and comprehensive framework to define Internet fragmentation, its intended and unintended causes, and its potential effects; (b) Collect and analyze case studies to fine-tune and complement this framework; (c) Establish shared principles, recommendations or codes of conduct that prevent fragmentation and preserve the open, interconnected and interoperable nature of the Internet.

Details on the PNIF activities can be found on the PNIF webpage.

Introducing the PNIF Framework for discussing Internet fragmentation.

The framework has been developed as a result of conversations, amongst other at the PNF webinars, that were driven by key questions such as what is fragmentation and how and where does it manifest, asked with the aim to find some level of commonality in the thinking and ongoing discussions about internet fragmentation.

Throughout these discussions people continued to speak to two areas, one fragmentation of the user experience, the other fragmentation of the technical layer of the Internet. An overarching point that came up in the discussions related to a possible fragmentation of the overall governance of the Internet. (the framework is explained [here](#))

With the framework the PNIF wants to provide a basis to continue discussion about internet fragmentation and unpack the different elements in greater detail, with the aim to develop a common understanding of the issue and be able to come to solutions and recommendations to different actors, to address internet fragmentation.

Unpacking the draft PNIF Framework - feedback & discussion

(The below summary paraphrases the feedback received during the session and suggestions made by participants. They do not constitute conclusions reached during the meeting.)

- The framework gives the opportunity to launch the debate, exchange views and review outstanding biases that one may have.

- The international community calls upon the internet community to help solve global and collective problems - such as climate change, pandemic prevention, and promoting the SDGs. Contributing to solving global issues, however, will require a shift from a solely individualistic approach to user experience to an approach that includes a human centric dimension and promotes collective values.

- There is no single type but a multitude of users. Different groups and categories of users face different challenges. This diversity should be reflected in the framework.

- Untargeted internet disruptions such as shutdowns, blocking and social media restrictions used by authoritarian regimes for political control affect all kinds of users including those wanting to use the internet for work or recreation.

- The internet is made up of a technical infrastructure (by some addressed as 'the public core of the internet') that need to collectively interoperate at a global scale to make the internet work: the naming, the routing, the forwarding, and the cryptographic infrastructure. The 'core' infrastructure is not the only internet infrastructure and other, new infrastructure may gain importance in the course of technical development. (for example the technology that allows the use of a social network ID to log into other services could be considered as a new underlying technology for other services).

- The routing of internet traffic via private infrastructure by big tech companies is an example of a long-term commercial activity that might lead to fragmentation if the investment in the own private infrastructure (cables, datacentres, etc) coincides with an underinvestment in transit infrastructure that allows users to get to other content.

- The governance of the internet infrastructure is decentralised with a hierarchy of independent multistakeholder organisations managing the different parts while working together to provide an open and interoperable internet. Fragmenting this governance framework may have disastrous effects.

- Some fragmentation of the user experience isn't going to result in technical fragmentation, while technical fragmentation will always result in broader fragmentation. Some forms of fragmentation may be devastating and long term, a framework should take into account the severity of the ramifications of anything happening at the technical layer.

- The answers on what is fragmentation and which aspects of fragmentation are most relevant are shaped by political views.

- Discussions on fragmentation and the future of the internet should move from an individualistic to an collective paradigm with regard to user experience; move from a model of stakeholder cooperation to a model of cooperation and mutual empowerment of stakeholders with regard to governance; address legal risks originating from organisations or infrastructure being subject to a single jurisdiction, as for example ICANN under California law.

- When further unpacking the framework and the different dimensions, it'd be helpful to identify at what point certain practices would constitute or qualify as fragmentation (e.g. impact or duration of shutdowns).

- From a purely technical infrastructure perspective the darknet are sites and information that can not be found through the regular search engines. As the information is available and reachable over the internet in some way through a set of protocols, it is not an example of fragmentation. However, if you broaden the definition of the internet's technical infrastructure and include search engines, then one could argue that darknet is a form of fragmentation as search engines are not picking up the information.

- The introduction of certificates by governments can interfere and cause fragmentation in the application space as some applications may to block the certificate. One should discuss how to deal with this situation.

- The notion of 'avoiding internet fragmentation' in the work around the GDC is different from the one discussed at the PNIF so far. The GDC is to some extent focused on fragmentation of the information and the need to come to a convergence of ideas, of knowledge and avoiding echo chambers - the framework does not capture this yet. It's recommended to include it.

- It is Important to identify instances where governments play a role (eg govs vs shutdowns) and promote multistakeholder and international cooperation.

- The Russian-Ukrainian war has accelerated trends of protection and nationalism, similar trends are being seen in the digital sphere as well (e.g. the rise of authoritarian internet models with citizens segregated from the rest of the global internet). This presents a real risk to the internet as we know it.

- Governments should be constantly encouraged to heed their human rights obligations and protect and promote the free flow of information, recognising access to the internet as a human right and refusing to resort to internet shutdowns.

- Large tech companies and their products may impact human rights. Human rights need to be centric in the development of products and policies.

- One participant identified the following reasons for internet fragmentation: 1) increasing weaponization and and militarisation of the internet which has become a new battlefield; 2) unilateral coercive measures in the digital world; 3) the non-cooperation of global digital platforms with law enforcement of countries regarding illegal content and investigation of cybercrime.

- Would a global declaration signed by all MS recognizing the internet as a peaceful environment for public good be confidence building enough and a solution to avoiding internet fragmentation ?

- It is important to also have a clear understanding of what is not internet fragmentation or a consequence of it (for example cybercrime, discrimination).

- The definition of and discourse around fragmentation should not be redefined to exclude things that are fragmentation but that we accept as acceptable (e.g. certain law enforcement action against harmful content). A 'this is fragmentation and this - if we like it - is not' discourse should be avoided.

- It might be necessary to qualify or better define the 'user'.

- Should fragmentation be held up against an ideal standard of what the internet experience should be like rather than what it is? The example of globally applied extraterritorial measures (eg global content takedown) may potentially go against certain human rights principles, but not fragment the user experience.

- There are ramifications of internet fragmentation on emerging technologies such as AI, IoT, Big Data. Restrictions on the free flow of information and data may exacerbate issues of fairness and bias in new technologies, or exclude people and nations.

The framework remains open for comments. The input from the session and will feed into further work and the discussion of the envisaged phase 2 of the PNIF.