IGF 2023

Policy Network on Internet Fragmentation

(PNIF)

PNIF Discussion Paper

(input to IGF 2023)

15 September 2023

Table of content

Table of content..... 1

1. Introduction..... 2
1.1. The IGF Policy Network on Internet Fragmentation..... 2
1.2. Setting the scene: the PNIF 2022..... 2
1.3. PNIF 2023 plan..... 4

2. Internet Governance and Coordination..... 5
2.1. Unpacking & prioritising..... 5
2.2. Recommendations for addressing fragmentation of Internet governance & coordination
2.3. Further areas for research to adopt best practice..... 9

3. Internet Technical Infrastructure..... 10
3.1. Unpacking & prioritising..... 10
3.2. Recommendations for addressing fragmentation of the Internet technical layer..... 11
3.3. Further areas for research to adopt best practice..... 12

4. Internet User Experience..... 12
4.1. Unpacking..... 12
4.2. Recommendations for addressing fragmentation of Internet user experience..... 18
4.3. Further areas for research to adopt best practice..... 19

5. Discussion & call for community feedback..... 20

6. Invite - PNIF session at IGF 2023..... 21

7. Work plan and Next steps..... 22

8. Acknowledgements..... 22

Annexe PNIF activities and resources..... 23
PNIF 2023..... 23
PNIF 2022..... 25

1. Introduction

1.1. The IGF Policy Network on Internet Fragmentation

Internet fragmentation is a complex issue. The many views, diverse opinions, different conceptualisations and definitions of what is and what is not internet fragmentation, or what fragmentation - in the context of the UN Secretary General's Our Common Agenda - should be avoided or addressed can hinder an open and inclusive dialogue, and discussions on common guidelines or principles.

The proposal for a Policy Network on Internet Fragmentation (PNIF) was born out of a community initiative launched by a multistakeholder coalition of civil society, business and technical community organizations in 2021 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 IGF Multistakeholder Advisory Group (MAG) confirmed Internet fragmentation as topic for an IGF intersessional activity that aims to offer a systematic and comprehensive framework, complemented by case studies, to define Internet fragmentation, its causes, and its potential effects and it aims to establish recommendations or codes of conduct that prevent fragmentation. The PNIF proposal envisaged a two-year work plan with focus in its initial year on establishing a systematic and comprehensive framework to define Internet fragmentation, its intended and unintended causes, and its potential effects.

1.2. Setting the scene: the PNIF 2022

In 2022 the PNIF webinars and discussions confirmed the diversity of opinions, and an attempt to deduct a common definition of internet fragmentation via a survey launched earlier in the year didn't prove successful. Through the discussions, however, emerged elements of a framework that could serve to guide and orient future discussions.

The draft framework for discussing internet fragmentation constructed by the PNIF was shared with the community ahead of and discussed during a PNIF session at the IGF annual meeting in Addis Ababa. The aim is to have a refined and more mature framework ready for a second phase of the PNIF, focused on identifying potential causes of fragmentation and defining solutions and policy approaches to avoid fragmentation.

A Framework for Discussing Internet Fragmentation

The overall goal of the framework is to serve as a general guiding and orienting tool for continuing the dialogue about fragmentation and bringing in more people and stakeholders. The framework should allow a more holistic and inclusive debate, and at the same time, create space for focused discussion and work towards concrete solutions, policy approaches and guidelines.

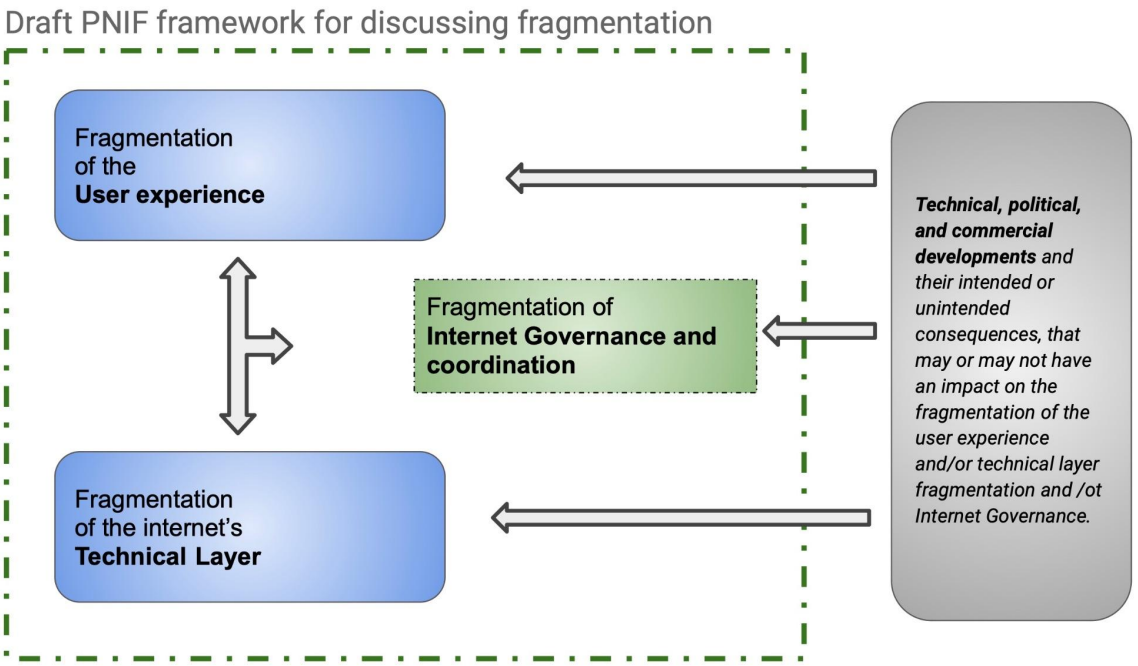
The Framework that emerged from the PNIF discussions conceptualises three key dimensions of fragmentation:

- ***fragmentation of the user experience,***
- ***fragmentation of the Internet's technical layer***, and
- ***fragmentation of Internet Governance & coordination***.

The Framework indicates that **technical, political and commercial developments** and their intended or unintended consequences may or may not have an impact on fragmentation.

The Framework captures potential **relationships and overlap** between the dimensions, between technical fragmentation, user experience fragmentation, as well as governance fragmentation.

The **Human rights framework** and the need to maintain a **free flow of data** could be used to evaluate measures that impact the user experience and assess if the measures enhance the user experience or have a negative impact and as such should be avoided. The **interoperability of the global internet infrastructure** is proposed as reference framework to assess technical fragmentation. The internet governance dimension aims to capture the commitment to the **Multistakeholder management** of the technical layer of the internet and the existence or lack of a **global framework** across multilateral and multistakeholder venues, governments and stakeholders **to address global internet policy issues** from a human rights and free flow of data perspective.



1.3. PNIF 2023 plan

The PNIF in 2023 intends to further unpack the PNIF framework via three parallel work streams on fragmentation of the user experience, fragmentation of the Internet's technical layer, and fragmentation of Internet governance and coordination.

The work streams work in an open and bottom-up manner to further unpack fragmentation and take a deep dive into identifying, prioritising, and prevention and addressing:

- identification : Identify which types of fragmentation and related actions pose the highest risks and should be addressed or avoided;
- prevention : Define practices, guidelines, and principles to prevent or address fragmentation.

The the combined work of the three work streams will constitute the PNIF 2023 outputs, which are envisaged to include:

- A refined and robust framework for discussing fragmentation, to provide increased clarity and common understanding about the diverse causes of fragmentation, their interrelation, impacts, and when fragmentation is most harmful and should be avoided.
- Recommended high-level overarching principles to avoid Internet fragmentation (building on the 2022 framework), to feed into discussions between policymakers

and stakeholders, in particular but not exclusively in the framework of Global Digital Compact (GDC) process.

- Concrete guidance and solutions for stakeholders to address fragmentation, including alternative solutions for problematic policies and behaviour that might lead to harmful fragmentation.

2. Internet Governance and Coordination

2.1. Unpacking & prioritising

Fragmentation of Internet governance primarily relates to the interactions between global Internet governance and standards bodies. When these bodies do not coordinate inclusively, it can and does result in fragmentation. This fragmentation can manifest in siloed or duplicative discussions and exclusion of specific groups from participation, resulting in decisions being taken without consensus from the global multistakeholder community. Fragmentation at the governance level can also create knock-on effects for fragmentation at the technical and user experience layers.

The Internet governance ecosystem is a complex network of interconnected bodies that work together in coordination and collaboration.

In terms of coordination, one body needs to receive updates on what another body is doing to understand how work streams may have reciprocal impacts. For example, if the IETF is developing a new standard or protocol, this shouldn't happen in isolation. It is valuable, and in some cases critical, to understand what is happening in standards development in interrelated technology areas (for example at the ITU-T[1]). It can also be important to understand deployment and implementation experience (for example from best practice sharing at RIRs and Network Operator Groups), and in turn, keep such bodies abreast of its work.

In terms of collaboration, sometimes two bodies (for example, ICANN and RIRs) need to work together on a shared, or overlapping, objective. To collaborate, bodies need to work together through a voluntary approach and adapt when responsibilities are not firmly defined under a clear mandate. It is in the interest of all stakeholder participants to see such collaboration carried out efficiently.

Duplicated and exclusive mechanisms, in the form of work items, initiatives, or bodies, harm coordination and collaboration across the Internet governance space, resulting in fragmentation at the governance layer.

[1] Note that for this purpose various standardisation organisations maintain liaison relations, joined mailing lists, and other kinds of coordination.

Avoiding duplicative mandates

Firstly, duplicative mandates reduce efficiency and inclusion. This can foster competition for legitimacy between bodies, contributing to fragmentation of the Internet governance ecosystem. This can lead to uncertainty for the community and potential divergences in approach taken by different stakeholders. There are two distinct paths that can lead to duplicative mandates. Such mandates can arise through scope creep, for example if one body starts taking up issues that already fall under a different body's mandate. Setting up a new body, which has an overlapping mandate to an existing body, also creates duplication.

Avoiding closed forums with closed/exclusive participation

Fragmentation can also occur at the governance layer through the creation of bodies or initiatives that do not allow for the full participation of the multistakeholder community.

When a new body or initiative creates, whether intentionally or unintentionally, a closed community, this excludes stakeholders. Inclusivity, transparency and accessibility are essential components of Internet governance bodies and initiatives - exclusive bodies contribute to fragmentation at the governance layer, as they encourage stakeholders to communicate in silos. Potential longer term effects of decisions to create new bodies or initiatives should be considered as well, particularly regarding making them fully integrative to all stakeholders from the start. As with duplicative mandates, closed bodies contribute not just to fragmentation at the governance layer, but can also lead to other forms of fragmentation, such as the Internet's technical layer.

Fostering meaningful inclusion is a particularly pertinent point in that regard. Some organisations and groups of stakeholders, especially in the Global South, are currently left out, or feel left out of Internet governance processes and bodies. Where processes create a sense of alienation, or present high barriers for key stakeholders to engage meaningfully, this can contribute to actions being taken elsewhere in competing or parallel fora and organisations or at the national level.

Taking action with the right measures and at the right level

Governance at the national level interacts with Internet governance at the global level in ways relevant to fragmentation. Individual governments' actions can lead to divergence in the rules applied to the Internet and its management, or undermine the bodies of Internet governance and standards development. Given the unique levers available to governments at the national level, actions have the potential to be detrimental to a single consistent global Internet experience if alignment on underlying basic principles is lacking. Procedurally,

if individual governments are not able to be fully and productively engaged with multistakeholder global governance, one outcome can be an increase in national measures, which in some cases undermine the principle of consensus as well as the legitimacy and effectiveness of global internet governance organisations.

To address this imbalance, global Internet governance bodies can take actions to empower these stakeholders who might otherwise go unheard. For example, by implementing specific global collaborative regulation procedures for the Internet ecosystem.

Additionally, there is a need for global Internet governance bodies and national and regional political bodies to engage more closely with each other. Such bodies might pass legislation that impacts the Internet, without realising the full implications or without consulting all stakeholders. On the other hand, internet governance and technical organisations may not realise the implications of their actions in national contexts, where they may not sufficiently enable input from a diverse array of stakeholders including governments. Early engagement with global Internet governance bodies could help to mitigate negative consequences which might arise. This engagement is important at the executive, legislative and judicial levels.

2.2. Recommendations for addressing fragmentation of Internet governance & coordination

1. Do not introduce further bodies into the Internet governance landscape….

The Internet governance system is complex, with the involvement of an array of different bodies: ICANN, IETF, the IGF and the ITU. Introducing new bodies into this already complex landscape can harm inclusion, as stakeholders, particularly those with less financial resources (like civil society and developing countries) do not have the resources to proactively engage with all of these bodies as it stands. Proposals to introduce new bodies within internet governance, such as the proposal for a DCF, risk fragmenting this landscape further. The perpetuation of bodies could cause stakeholders to make difficult decisions about where to engage, siloing them from discussions taking place elsewhere. Proposals to introduce new bodies have to be evaluated/weighed against the risk of fragmenting the landscape further.

Proposals for additional Internet governance bodies also risk duplicating existing mandates. In the case of the DCF proposal, the Internet Governance Forum already holds responsibility for bringing all stakeholder groups together on an equal footing to discuss policy issues related to Internet governance.

2. …. but, improve coordination between existing Internet governance bodies.

Nonetheless, few clear coordination mechanisms exist between existing Internet governance bodies. This opens up the risk that mandates could be duplicated, and false gaps identified when in actuality, a particular body has it within their remit to take forward work in a particular area.

To address fragmentation of governance at a systems level, steps can first be taken within existing Internet governance organisations. These bodies should proactively seek improvements in the way they operate, with an expectation that improved organisational governance measures will in turn improve the way each organisation interacts with other organisations. Better internal processes and governance are likely to lend themselves to better outreach and coordination, which would likely result in better information sharing and the deconfliction of mandates.

Coordination mechanisms are important both at the level of detailed work in Internet governance and technical organisations, as well as at the level of strategic direction.. Such a mechanism at strategic level could help to clarify areas where mandates may overlap, and therefore serve to clarify or eliminate any existing duplication. In addition, the introduction of any mechanisms must be institutionalised so that coordination and communication are not over reliant on specific individuals or informal networks.

3. To avoid siloed public policy discussions regarding Internet governance, all Internet governance bodies must be fully inclusive to stakeholders and enable meaningful multistakeholder participation.

Ensuring the multistakeholder community can meaningfully participate in Internet governance bodies is key to ensuring that the Internet's governance layer does not fragment. As extrapolated on above, the siloing of different groups of people into different bodies can hurt governance processes, by excluding important perspectives from discussion either through resource constraints or by lack of mechanisms for full multistakeholder participation.

This is not simply a risk with the potential introduction of new bodies or mechanisms into the Internet governance landscape. Existing Internet governance bodies also need to consistently evolve to ensure they are enabling the meaningful participation of all stakeholders in practice. For example, certain processes in Internet governance are quite technical. To ensure all stakeholders across regions and groups can meaningfully participate in such processes, Internet governance bodies need to provide relevant resources aimed at upskilling newcomers and invest resource in capacity development initiatives - simply saying that all can participate is not enough.

Equally, the UN must take the same approach when it initiates processes related to Internet governance. There needs to be a recognition from UN officials that multistakeholderism is core to the effective functioning of the global Internet, and as such, flexibility to create multistakeholder processes when it comes to negotiating, agreeing to and implementing principles and mechanisms that affect Internet governance. In this regard, UN officials can look to the IGF in particular to solicit examples or ideas for best practice on enabling effective multistakeholder participation.

4. **Existing global Internet governance bodies must engage more closely with national governments.**

Engagement between national governments and global Internet governance bodies must increase. In particular, to encourage governments to include all stakeholders in their policy work on Internet governance and empower multistakeholder participation within these countries. In addition, such engagement can help global Internet governance bodies to understand the motivations behind, and provide feedback on, the implications national legislation could have on the global Internet governance ecosystem. In addition, increased engagement from global Internet governance bodies at the national and regional level can also equip national governments and regional political bodies to meaningfully participate in the complex Internet governance ecosystem.

2.3. Further areas for research to adopt best practice

This analysis and the corresponding recommendations are high-level, focused on principles. However, further work should be undertaken to examine what specific best practice could be applied to the Internet governance space to improve coordination and mitigate

fragmentation of the governance layer. Mechanisms ripe for further exploration, to assess best practice but also lessons learned, include:

- OECD's Best Practice Principles on the Governance of Regulators
- The ITU's G5 collaborative regulation

3. Internet Technical Infrastructure

3.1. Unpacking & prioritising

Fragmentation is not a clearly defined term and trying to arrive at a definition that can be operationalized is a topic that needs further exploration. The Internet is made up of a technical infrastructure that collectively interoperates at a global scale so that data (information) is reachable and can be transported over the Internet. **Fragmentation of the Internet's technical infrastructure thus relates to a range of challenges to this interoperability** at the technical transport layer that makes the Internet work, and upon which applications and services are reliant.

The technical infrastructure underpinning the Internet is made up of a diverse range of technologies, which vary significantly in their role and importance to the functioning of the Internet overall. While challenges to interoperability that contribute to Internet fragmentation can occur at a variety of points, frameworks such as the *Critical Properties* from the Internet Society, or the *Public Core* as introduced by the Global Commission on Stability in Cyberspace, or the *Technical Success factors* of the Internet expose priority components where fragmentation occurring would have more serious negative implications. When we move away from the implementation of these frameworks, then it is likely that some form of fragmentation is enabled.

Technical layer fragmentation is not and should not be confused with :

a. Decentralisation in the management of the Internet infrastructure (e.g. IP resources, DNS); On the contrary, the shared responsibility for managing Internet infrastructure creates resilience, provided that common approaches (for example for Internet identifiers such as the Domain Name System) are maintained.
b. Lack of connectivity generally, or between specialised networks which can have multiple causes; e.g private networks set up for security reasons
c. The evolution of the internet and related technologies; because the Internet is not static.

The following practices may impact the Internet's interoperability and as such lead to a fragmentation of the technical infrastructure:

a. A negative impact on the internet's critical properties, moving away from fundamental Internet design principles, or interference with the public core of the internet;
b. The concentration or consolidation of traffic being routing outside of the public interoperable Internet; The Open Architecture based on open Standards leads to the possibility of decentralised deployment and leads to interoperability. Closing the architecture has fragmentary effects. In the routing space, an increasing amount of traffic is facilitated over private proprietary networks, leading some to question whether we are witnessing the "death of public transit". In the application space that can be observed more easily. For instance, be seen with messaging, where users cannot communicate between various brands of proprietary messaging apps.
d. Interventions in the technical infrastructure layer to mitigate issues in the content layer.

3.2. Recommendations for addressing fragmentation of the Internet technical layer

1. **Recognise that there are critical properties of the internet/public core that require multistakeholder protection**

    - Consider defining: Digital public infrastructure, public core, digital public goods
    - Commit to not attacking/impairing the core and critical properties
    - Commit to protecting the critical properties of the internet
    - Continued decentralised management and governance of IP address space (link to governance fragmentation)
    - Protect the current root system

2. **Measurement to monitor the extent and nature of different types of technical fragmentation as the Internet evolves.**

    - Coordination and information sharing on measurements of adoption / use of key elements of the shared public core of the internet including standards.

- Measurements of reliability and support reachability by addressing peering disputes and routing misconfiguration (unintended) and shutting off access (intended). An example is the Dashboard on Internet resiliency and concentration by the Internet Society (pulse.internetsociety.org); complementing measurements and academic research needed.

3. **Critically assess and avoid technical proposals (in standards and technology development) which reduce interoperability or otherwise would take the Internet away from the properties and design principles which have led to its success.**

4. **Protect the multistakeholder approach**

   - Promote inclusive policymaking that integrates consideration of technical expertise/impact of policies on critical properties of the internet (impact assessments could be helpful here)
   - Avoid policy interventions and regulation that would undermine technical standards setting and implementation of consensus-driven standards.
   - Address the impact of sanctions or interventions with the infrastructure of the internet by creating space for discussion and collaboration on these issues in multistakeholder fora
   - Support liaison relationships between technical internet organisations such as standards bodies, regional internet registries, ICANN, and others.

3.3. Further areas for research to adopt best practice

[to be elaborated pending further input]

4. Internet User Experience

4.1. Unpacking

Fragmentation of the user experience can be understood as the phenomenon by which different end-users of the Internet, when trying to perform the same action online, are presented with different content, options or interfaces. This happens normally as the consequence of using different client-side instruments (devices, applications), different server-side platforms (search engines, social media), different languages and ways of expression, and also, as the consequence of being located in different parts of the world; moreover, this is often the result of per-user customizations applied by the services that are being used.

Many of these differences are actually beneficial, facilitating the user's success by providing a more familiar and tailored experience. However, **when such fragmentation is forced upon the end-user by other parties, or when it hampers the communication among end-users and their ability to access content and services, it can deny the advantages and the freedoms that the Internet is supposed to offer.** This is the kind of fragmentation that is detrimental to an open internet as a whole, and which must be addressed.

While coordination and interoperability at the technical and governance layers is a requirement for the Internet to exist, significant variance in user experiences throughout cultures, jurisdictions, devices and platforms is normal; it has always existed since the Internet was created. In terms of countries, it allows for the preservation of national customs and values; in terms of platforms, it allows for differentiation and competition. However, this variance should not deny the basic rights of end-users, both in terms of communication rights and of the ability to choose freely their services and applications.

In recent times, two major trends have been increasing the amount of fragmentation observed at the end-user level.

1. **Companies** - especially Internet platform providers - pursued the profiling of users and the customization of services and advertising, and introduced measures (user interface designs, terms and conditions, business and technical practices) that restrict their ability to move to competing services or to interact with third party

services and products and with their users, when these parties do not have commercial agreements with the platform, or when the platform owns a competing product.

2. **Governments** increased the amount of national and regional legislation addressing Internet activities, industries and content; from a user experience fragmentation - this generated a broad spectrum of effects that include forcing global companies to store data in-country in a way that is not harmonised with global best practice (and therefore reduces data flows) making specific websites and content, including media outlets, unavailable to end-users in the country.

In the end, the definition of “Internet fragmentation at the user experience level” is necessarily broad, including a great fraction of what happens over the Internet. Narrower definitions have been attempted, but without reaching consensus; different stakeholders find harm in different parts of the trends described above. Often, fragmenting measures are introduced as a response to other harms, and the loss of uniformity in Internet access is considered as an acceptable price to pay to counter these harms; however, this is by definition a policy compromise which may be assessed differently according to the views and interests of each stakeholder group, and to the culture and values of each nation.

Thus, our focus should be those measures taken by stakeholders that are disproportionate in the harm that is caused to the user and service provider, in terms of their control over the experiences that they consume or create online, which if replicated globally would harm an interoperable, free, and open Internet. A “case by case” approach may be necessary to determine when specific regulatory, technical and business trends that introduce variance in end-user experiences should be considered harmful to the Internet as a whole. Any global solution should allow for a reasonable degree of national differentiation (taking into account local values and cultures), but must be based on democratic procedures and multi-stakeholder consensus, building on the principles of decentralisation and devolution.

One method to evaluate these trends for their fragmentary potential may be to create a crude conceptual model to distinguish between **equal** and **equitable** user experiences.

“Equitable”, or outcome-driven experiences, might focus on general issues that affect user interactions with the internet more broadly (e.g. the digital divide, internet speeds and meaningful access, net neutrality, linguistic diversity and localization, accessibility for disabled individuals etc.) - which is more **aspirational** in its policy implications. In doing so, we can carve this portion out for discussions in related areas, acknowledge its importance

and fragmentary potential, but avoid having these issues interfere with the more targeted discussions on fragmentation.

“Equal” experience discussions are more basic in nature. With certain assumptions about the typical internet user (in terms of connectivity to the internet, effective speeds, understanding language etc. as covered above) we can focus on common high-priority harms that can affect the user experience as described below, which have the common characteristics of directly or indirectly stripping away user control over their digital experiences, and controlling applications and content providers in a way that leads to inconsistencies and dissimilarities among platforms or regions.

Prioritising

Given the varied and controversial nature of user experience fragmentation trends, in global policy venues it has been hard to agree on a shared set of priorities.

The private sector, especially the global Internet industry from the United States, has been focusing their objections on the fragmentation introduced by new legislation by multiple countries and by the European Union. This includes data localization laws (sometimes also privacy laws), attempts to introduce lawful interception of personal communications by law enforcement agencies (especially if they somehow undermine encryption), and any further requirements that create costs and liabilities and introduce the need to differentiate the service by the end-user’s geographical location, such as national content blocking and content moderation requirements.

On the other hand, governmental and parliamentary action - though very variable depending on the country - has generally focused on countering negative social and economic effects attributed to the platforms, ranging from disinformation to oligopolies; and on making specific content unavailable under multiple motivations, from security to protection of minorities and to the enforcement of fiscal law, but also, in certain countries, for purely political reasons.

Civil society tends to hold a wide variation of priorities and opinions; for example, laws that attempt to counter the circulation of child sexual abuse material are often criticized by digital rights groups, however the same measure may be praised by children’s rights associations.

It is hard to identify a common set of problems and priorities all stakeholders agreed upon . Therefore, as an alternative approach, we discuss specific problems one by one, to then, when some common and broadly acceptable principles start to emerge, try to foster consensus across stakeholders.

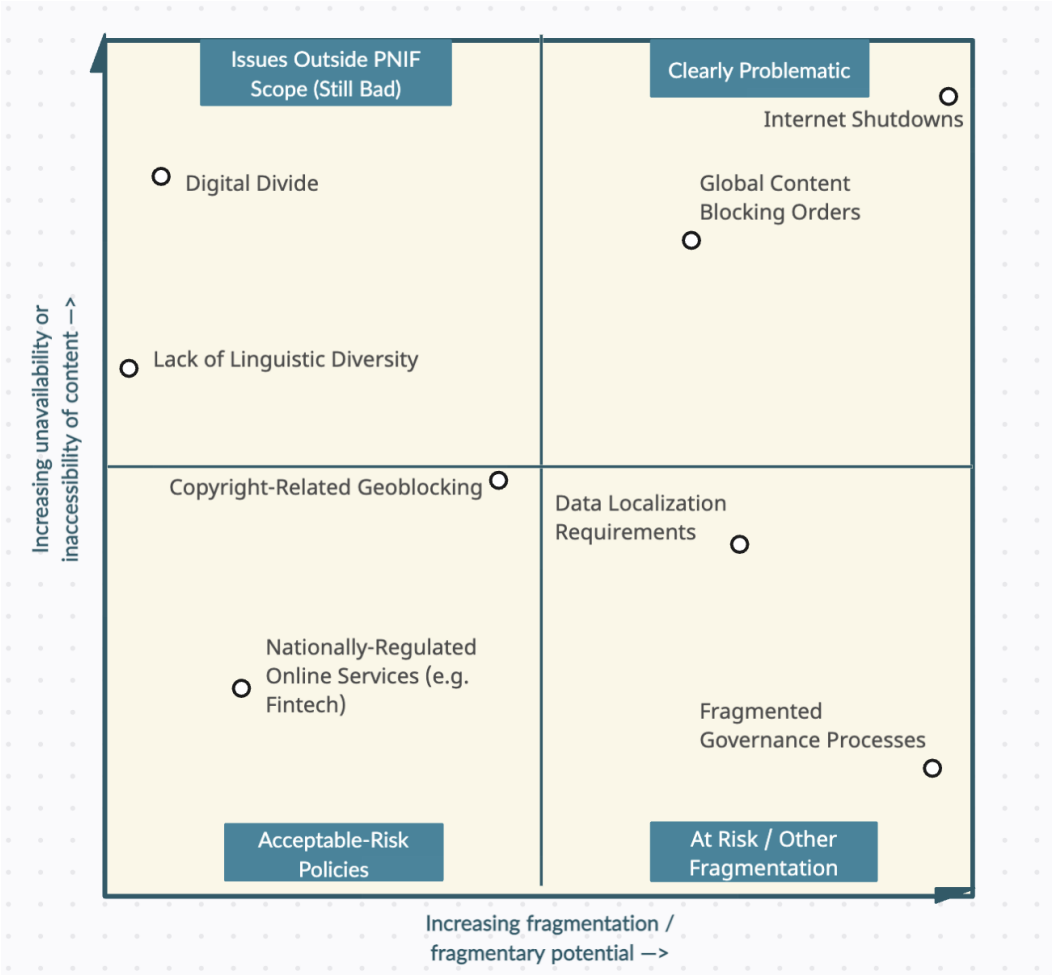
The following are proposed examples of high-priority “bad” fragmentation (using a type of “per-se” rule - there is no good justification for any of these as the harm they cause is principally worse than the harm they are trying to address), due to their disproportionality, deliberate nature, and traits of controlling online experiences (whether that be by targeting the users directly, or those that provide content and services online):

- 1. Internet shutdowns. When all connectivity is turned off in a given city, region or country, or for all the users of a major ISP, the Internet simply ceases to exist for those who live there. As such, this is the worst case scenario for users, as it denies any usage of the Internet; this is never an acceptable response.
- 2. National content takedown and blocking orders having global effect. No country should have unilateral jurisdictional reach on what content or resources are available beyond its borders regardless of the issue in question (e.g. defamation laws may differ, as may IP laws). Even in the most egregious of cases (e.g. CSAM), local notice-and-takedown, global cooperation and common reporting, and harmonisation at multilateral levels through treaty instruments is a more systemically robust approach. When the takedown of resources (e.g. domain names, WebPKI certificates) would make content and services globally unavailable, it should only happen according to globally agreed principles. When legal measures from one jurisdiction (e.g. court orders around content or domain blocking) affect global service providers, the providers should implement them so that they only apply to requests coming from that specific country.
- 3. Digital protectionism via lack of competition and user choice in digital markets. This includes governments trying to favour national, State-owned services for communications and Internet access, outlawing more modern and/or private alternatives such as VoIP services or VPNs. This also includes global platforms trying to lock users into their set of services and hampering the birth of alternative local services and applications.

Other types of potentially negative fragmentation (that may need slightly more analysis into the effects rather than a per-se conclusion):

- 4. National content takedown and blocking orders, or other practices that incentivise censorship and self-censorship, that have no global effect, but are designed to stifle free information and hide politically sensitive content, and thus damage the human rights of the end-users from that country. It is thus necessary to tell blocks that are actually supporting the safety and security of users (e.g. against malware, or websites selling counterfeit medicines) or are necessary to protect third party rights (e.g. against child sexual abuse material or the illegal propagation of defamatory material) from those who are just aiming to deny political rights to the citizens of the country.
- 5. Violations of network neutrality. Throttling, zero-rating and other similar mechanisms affect the usage of the Internet and can make the connection unusable, limiting or removing the possibility for end-users to freely choose the services and content that they want to enjoy. While there can be technical cases in which some traffic discrimination is necessary, for example to prevent denial of service attacks or to ensure minimum service levels to everyone when the network is congested, these situations should be clearly limited and defined, avoiding any other breach of network neutrality motivated by commercial or political reasons.
- 6. Geoblocking or content differentiation that derives from the overzealous protection of intellectual property rights, especially if affecting content which has strong cultural value or which has no significant commercial value in the countries where it is blocked.

The following is a rough (example) matrix to help kickstart what falls where, and entails that we should be focusing on issues that are at (or close to) the top-right quadrant, practices or measures that are clearly problematic as they deny (groups of) internet users the advantages and the freedoms that the Internet is supposed to offer**.** In the top-left quadrant are issues related to the exclusion of groups of people from meaningful Internet access (from being or becoming Internet users). They often have diverse causes and cannot be traced back to deliberate practices or measures intended to exclude internet users from certain content or services. The bottom-right quadrant focuses on fragmentation issues covered by analysis of the other layers as well (technical and governance) that may have indirect or longer-term tendencies towards fragmentation of the user experience as well.



4.2. Recommendations for addressing fragmentation of Internet user experience

We propose the following principles to address the harms identified above resulting from fragmentary behaviours.

1. The Equality Principle

Every user of the Internet, regardless of where they are based, should - as a starting point - be able to access any content, resources, applications and services that are intended

(whether unconditionally, or subject to any fulfillable conditions, commercial or otherwise) to be made publicly and globally available, in the same manner.

2. The Enhancement Principle

Measures to enhance the user experience by making it more relevant, meaningful, understandable, secure, or accessible, and that are requested by the users themselves (e.g that content is available in different languages) so as to, in effect, align the user's experience of the Internet with their own intentions or desires - should not be considered as "bad" fragmentation that contravenes the first principle, notwithstanding the potential effects on uniformity.

3. The Impact Assessment Principle

Any measure - whether by governmental, private sector, or technical actors - that may have a directly intended effect (or creates the incentive) to diminish or render ineffectual the first principle, must be evaluated prior to its introduction or implementation to ensure that such a measure is proportionate, addresses a legitimate harm, is respecting of human rights, and follows democratic procedures with multi-stakeholder involvement.

4. The Harmonisation Principle

Fragmentation that may be driven by diverse national regulatory or legislative approaches to protect the human rights or legitimate interests of Internet actors (such as the protection of privacy, the protection of minors, parody or fair use of intellectual property etc.) can be avoided through cooperation and multilateral instruments (informed by multi-stakeholder consultation) that set globally-applicable baseline standards and protections of those rights and interests, focusing national intervention on the issues for which no adequate protection has been established at the global level yet.

5. The Free Choice Principle

No user of the Internet should be coerced or unduly incentivised to use a particular platform, technology, or service provider - especially in order to provide or access content, resources, applications or services on the Internet that would not have otherwise been made possible or available to them (or would have been possible or available in a manner that renders the experience fundamentally different due to lower quality or greater barriers to entry). Users should be able to choose the applications, instruments and service providers

that they use and should not be subject to unfair conditions deriving from dominant market positions, lock-in and network effects.

4.3. Further areas for research to adopt best practice

[to be elaborated pending further input]

5. Discussion & call for community feedback

IGF Policy Network Internet Fragmentation

Submit your feedback on the PNIF 2023 Discussion paper at
PNIF-2023@intgovforum.org

Closing date consultation is Sunday 15 October
Recommended deadline **Sunday 1 October***

Submissions will be posted on the PNIF webpage

**to feed into the PNIF session at IGF 2023*

6. Invite - PNIF session at IGF 2023

Policy Network Internet Fragmentation
Tuesday 10 October

09:00-10:30 am UTC+9
IGF2023, Kyoto, Japan

Draft Agenda

1. Welcome & introductions *5 minutes*

2. The IGF Policy Network on Internet Fragmentation (PNIF) *20 minutes*

    a. Purpose and work plan
    b. PNIF 2022 and PNIF Framework for Discussing Internet Fragmentation
    c. PNIF 2023 highlights and general findings

3. Presentation of findings and recommendations by track *30 minutes*

    a. Internet Governance and Coordination
    b. Internet User Experience
    c. Internet Technical Infrastructure

4. Discussion and community feedback *25 minutes*

5. Summary and next steps *25 minutes*

Register for IGF 2023
Registration deadline for on and offline participation: 3 Oct.
Remote participation details will be made available closer to the event.

7. Acknowledgements

This PNIF discussion paper is the product of the collaborative work of many, who participated in PNIF webinars and virtual meetings, or provided input on the mailing list.

This PNIF discussion paper would not have been possible without the valuable work of three dedicated drafting teams:

- **Drafting team 'Internet governance and coordination':**
  Rosalind KennyBirch, German López Ardila, Ian Sheldon, Bruna Martins dos Santos, et al.
- **Drafting team 'Internet technical infrastructure'**:
  Olaf Kolkman, Marek Blachut, Sheetal Kumar, et al.
- **Drafting team 'Internet user experience'**:
  Izaan Khan, Vittorio Bertola, Sheetal Kumar, et al.

Special thanks to the expert discussion-leads of the three PNIF webinars

- **PNIF webinar 1 - Internet governance and coordination**, 16 May 2023
  Anriette Esterhuysen, Wolfgang Kleinwächter, Susan Ness, Raquel Gatto
- **PNIF Webinar 2 - Internet user experience**, 24 May 2023
  Farzaneh Badii (Digital Medusa), Marielza Oliveira (UNESCO), Zach Rosson (Access Now)
- **PNIF Webinar 3 - Internet technical layer**, 27 June 2023
  Olaf Kolkman (Internet Society), Mirja Kühlewind (IAB)

Overall coordination of the IGF PNIF 2023:
Sheetal Kumar, PNIF co-facilitator
Bruna Martins dos Santos, PNIF co-facilitator
Wim Degezelle, PNIF consultant IGF Secretariat

A **PNIF Multistakeholder Working Group of Experts (MWG)** provided advice on substance scope and implementation of the policy network. MWG composition.

Annexe PNIF activities and resources

PNIF 2023

The PNIF organised three intersessional webinars on the dimensions in the internet fragmentation discussion conceptualised in the *PNIF Framework for Discussing Internet Fragmentation* - Internet Governance and Coordination, Internet User Experience, and the Internet Technical Layer - that emerged as output from the PNIF discussions in 2022. These webinars gathered broad community views to unpack, prioritise, and address fragmentation and informed the drafting teams that produced the first draft of this 2023 PNIF discussion paper.

PNIF 2023 Webinar 1, Internet Governance and Coordination

16 May 2023, 13:00-14:30 UTC
Recording https://youtu.be/xFPIoxBxXOM

Discussants: Anriette Esterhuysen, Wolfgang Kleinwächter, Susan Ness, Raquel Gatto.
Coordination: Sheetal Kumar, Bruna Martins dos Santos, Wim Degezelle.

Agenda

1. Introduction: Brief overview of the PNIF and PNIF Framework for Discussing Internet Fragmentation
2. Discussion: Fragmentation of Internet Governance and Coordination
    - Unpacking: What is and what is not fragmentation of Internet governance and coordination?
    - Prioritising: Which manifestations of fragmentation Internet governance and coordination pose a risk and should be avoided or addressed?
    - Addressing: What practices, guidelines, and principles could help to address fragmentation of internet governance and coordination?
3. Conclusion

PNIF 2023 Webinar 2, Internet User Experience

24 May 2023, 17:00-18:30 UTC
Recording: https://youtu.be/tn7hRw9xtGQ

Discussants: Farzaneh Badii, Marielza Oliveira, Zach Rosson.
Coordination: Sheetal Kumar, Bruna Martins dos Santos, Wim Degezelle.

Agenda

1. Introduction: Brief overview of the PNIF and PNIF Framework for Discussing Internet Fragmentation
2. Discussion: Fragmentation of Internet User Experience
    - Unpacking: What is and what is not fragmentation of Internet user experience?
    - Prioritising: Which manifestations of fragmentation of the Internet user experience pose a risk and should be avoided or addressed?
    - Addressing: What practices, guidelines, and principles could help to address fragmentation of the Internet user experience?
3. Conclusion

PNIF 2023 Webinar 3, Internet Technical Layer

27 June 2023, 12:00-13:30 UTC
Recording: https://youtu.be/vAelE5gmsAU

Discussants: Olaf Kolkman, Mirja Kühlewind.
Coordination: Sheetal Kumar, Bruna Martins dos Santos, Wim Degezelle.

Agenda

1. Introduction: Brief overview of the PNIF and PNIF Framework for Discussing Internet Fragmentation
2. Discussion: Fragmentation of the Internet Technical Layer
    - Unpacking: What is and what is not fragmentation of the Internet technical layer?
    - Prioritising: Which manifestations of fragmentation of the Internet technical layer pose a risk and should be avoided or addressed?
    - Addressing: What practices, guidelines, and principles could help to address fragmentation of the Internet technical layer?
3. Conclusion

PNIF 2022

IGF 2022 Policy Network on Internet Fragmentation Output

PNIF 2022 Output Report
Executive Summary

PNIF 2022 Workshop at IGF2022, Addis Ababa

30 November 2022, 6:30-8:00 am UTC
Summary

PNIF 2022 Webinar 1: What does Internet fragmentation mean to you? Identifying fragmentation and key stakeholders.

Meeting recording
Summary

PNIF 2022 Webinar 2: What can be done about Internet fragmentation, and who should be doing what?.

Meeting recording
Summary