Regional Roundtable

Internet Fragmentation and Human Rights in Europe

Session date: 12 December 2023

Background

The availability of a global open, interoperable, reliable, and secure Internet is necessary for the exercise and enjoyment of human rights in the digital age. However, these basic characteristics of the internet are currently under threat. There is a lack of understanding of the issue of internet fragmentation and the capacity to counter such threats, particularly among civil society. Countering threats to an open, interoperable internet effectively requires region-specific understandings. Despite this, current discussions on internet fragmentation have been largely siloed.

To address this gap, GPD is convening a set of stakeholders from the private sector, policymakers, and civil society for a series of roundtable discussions catered to a specific region. The aim of the roundtables is to (1) advance awareness and common understanding of internet fragmentation threats in key regions and; (2) to identify opportunities to counter them.

Session Summary

The first roundtable took place in December 2023 and focused on internet fragmentation within the European context. The roundtable convened around 30 stakeholders from across the internet governance landscape - including representations from the private sector, technical community, policymakers, standard development bodies, and civil society.

The discussion highlighted two trends within the EU: its commitment to support the unity of the internet versus its efforts to achieve digital sovereignty and reassert itself as a powerful player in the broader internet ecosystem. Participants came to a consensus on the need to address this tension between these two efforts to avoid internet fragmentation.

From the discussion, a set of suggested best practices and next steps for how the internet governance community can come together to prevent fragmentation and promote EU values and human rights within internet governance emerged. This included the importance of building the capacity of policy makers and civil society

organisations to identify threats to an open and interoperable internet as well as engage in relevant discussions. In addition, it was suggested that stakeholders focus on the core elements of the internet that we want to protect and preserve rather than focusing on defining internet fragmentation as a concept. For this, a principle-based approach grounded in human rights and that commits to protecting the critical properties of global connectivity is recommended.

Session Overview

Panel 1: Definitional clarity and context

The first panel session aimed to introduce internet fragmentation as a concept and specifically, whether - and if so, how - it has manifested in the European context.

Beginning with the question of how to define fragmentation, panellists emphasised the value of having a narrow focus particularly when discussing the issue with policymakers. Panellists also explored the intersection of politics and internet governance, and the politicisation of the internet's core - or of the fundamental internet technical functions that keep the internet together, such as the domain name system and the addressing system. Specifically, the panellists focused on the digital sovereignty discourse promoted by current EU leadership and how this could lead to fragmentation. Concerns were raised about the impact of regulations on global connectivity, trust, and governance, as well as the potential fragmentation driven by divergent standards and regulations across jurisdictions around the world.

Participants agreed that the community would benefit from a definition of the internet that recognises the innovation happening in the broader digital ecosystem that is dependent on the core technical infrastructures. However, panellists also cautioned that focusing on defining fragmentation can be a distraction from addressing the real issues at hand.

Lastly, panellists discussed the issue of sovereignty and its association with territorial boundaries. There was agreement on this being a part of the EU's political discourse that is contributing to internet fragmentation: the focus on strategic autonomy when implemented at the technical level of the internet is incompatible with a global internet. In other words, European strategic autonomy cannot happen without fragmentation within the context of the internet, and this is something with which policymakers must grapple.

Key takeaways

Having definitional clarity is essential for addressing the issue of fragmentation in the European context; however, participants recommended focusing on defining what we are trying to protect - an open, interoperable and secure internet - rather than fixating on defining fragmentation. A narrower definition focused on the

technical elements underpinning the internet allows for more focused discussions. Particularly within the context of efforts by the EU to achieve 'digital sovereignty' - a contested term in and of itself - focusing on the elements of the internet that make it the network-of-networks would allow for more productive, solution-oriented discussions.

Participants also noted that the internet is at risk of being fragmented by the EU's efforts to achieve strategic autonomy in areas like cyber security or artificial intelligence due to policymakers - among other stakeholder groups - taking the internet for granted and/or failing to understand the significance of global connectivity.

Lastly, panellists noted that there is a role for stakeholders - particularly civil society and the technical community - to play in raising awareness of this issue, and promoting the values of an open, interoperable internet, within broader geopolitical dynamics that underpin the EU's quest for 'strategic autonomy'.

Panel 2

The second panel session raised concerns about the impacts of regulatory approaches on internet fragmentation, user experience, economic and commercial ambitions, and the EU's commitment to human rights.

Participants discussed whether it is possible for the EU to balance its geopolitical ambitions with its strong commitment to upholding human rights. One panellist warned that while there may not be overtly fragmentary proposals being put forward in the EU, there is a risk of "death to the internet by a thousand cuts" with incremental changes ultimately leading to fragmentation. Participants noted that this is especially surprising coming from the EU.

A second question with which panellists grappled was whether to consider the wider digital ecosystem when discussing fragmentation or to have a narrower focus on the technical layer of the internet. Should commercial and economic fragmentation be considered? To what extent is what happening in the European context a reaction to broader global trends versus being internally driven?

Key takeaways

There was broad agreement on there being both intentional and unintentional/divergent interests within the broader geopolitical climate in Europe. Participants noted that we no longer live in a multilateral system where a spirit of togetherness and openness presides and as such, efforts to promote such values can feel like an uphill battle. While there is a discursive commitment to an open and interoperable internet at the EU, this stands in stark contrast to its efforts to reaffirm its sovereignty in the digital realm.

Participants also noted that there is a risk of over regulation and protectionism in the EU. The risk is that it goes 'too far' and regulates that which it doesn't fully

understand or without expert input. Some regulatory overlaps will be inevitable, and some regulation will take time for compliance to result in harmonisation across the continent, but policymakers need to consider these complexities when developing legislation.
However, it should be noted that the problem is not with regulation per se, but with certain types of policies, such as interconnection agreements that could impact key elements of the internet. Many such policies are also a reaction by the EU to regulations coming from other nations; for example, the DNS4EU initiative emerged as a reaction to the perceived market dominance of American companies in the internet resolver market and global trends towards 'sovereign' internet. The market dominance of key players - and the policies that have facilitated their growth and entrenchment - can be a driver of fragmentation, even when the regulation itself aims to do the opposite.

It is therefore important to consider a range of factors, including market forces, when developing digital policy. The risk is that such policies could, cumulatively, fragment the internet. Such regulations may come from Europe, or from efforts by other countries to apply similar regulations. Some policy makers demonstrate a lack of understanding of the importance of global standards for the EU, society, and for human rights. An example is the criticism of ETSI and its global participants by an EU Commissioner, which in reality is a strength for Europe in influencing global standards rather than a threat to the EU.

Concurrently, certain narratives and rhetoric are damaging and can be misused as well as buttress fragmentation prone, state-centric narratives outside the EU which itself contributes to fragmentation.

There are some positive developments: the passage of the European Digital Rights and Principles Declaration signed by all three EU policymaking organs reaffirms the EU's commitment to a human-centric vision for the digital ecosystem. The EU has also taken active steps towards supporting the unity of the internet, as seen in its exerting political capital in organisations like the International Telecommunications Union (ITU) and in bilateral agreements.

Participants concluded that we should consider measuring the incremental steps that are leading to internet fragmentation. There are some tools including the Internet Society's internet resilience index, as well as the Internet Impact assessment toolkit that could be built on. Participants also noted the importance of utilising internet governance processes for the communication of key messages regarding an open internet. It was suggested that the engagement of the technical community in these have been lacking so far. Additionally, for policymakers, there is a need to consider individual legislative initiatives holistically: what is the regulation about? What is the problem to be solved? What implications will this policy have on the broader digital ecosystem?

Takeaways

1. **Stakeholders must not take the internet - and especially the characteristics that allow it to interoperate and function as a network of networks - for granted. It is particularly important that governments consider these characteristics when developing and implementing regulatory interventions.**

2. **A principle-based approach grounded in human rights and that commits to protecting the critical properties of global connectivity is needed. These commitments need to be specific and tied to concrete actions.**

3. **There is a broader need across stakeholder groups to ensure that the core technical elements of the internet - such as global standards, domain name systems, identifiers, etc. - are not politicised.**

4. **Further research is needed to further elaborate on and 'connect the dots' more clearly between policy discussions and the technical components of the internet.**

5. **There is a need to reaffirm strong commitments to the multistakeholder model of governance of the technical layer of the internet and to commit to multistakeholder engagement in policymaking on all other issues pertaining to internet governance/digital governance.**

6. **Stakeholder communities must work together to overcome silos in the internet governance landscape, particularly at this critical juncture where the outcomes of several processes (including WSIS+20, NetMundial+10, Summit for the Future, etc.) have the potential to accelerate or decelerate internet fragmentation by undermining or reaffirming the multistakeholder model of governance.**

7. **Policy solutions and legislation must take a comprehensive and holistic approach to understanding the potential impact of regulatory frameworks on the internet. To this end, stakeholders must be meaningfully engaged in policy development, with the view to identifying threats to an open internet - particularly as these might be inadvertent.**

8. **There is a broader need for Europe to take an end-user driven approach that focuses on addressing potentially fragmentary trends.**

9. **There is a need to develop and implement means of measuring the incremental steps that are leading to internet fragmentation.**

10. **The EU needs to take a more balanced approach to policymaking to prevent its geopolitical and commercial interests from negatively impacting an open internet**

Recommendations

All stakeholders

- Agree/identify the key elements of the internet for which we are advocating to protect and safeguard. This includes the core technical elements of the internet - such as global standards, domain name systems, identifiers, etc.
- Commit to protecting these elements and ensuring that they are not politicised.
- Conduct further research to understand and 'connect the dots' between policy discussions and the technical components of the internet.
- Commit to developing methods for measuring the impact of regulatory proposals on the technical architecture of the internet before they are adopted and implemented. There is a need for a framework for understanding potential threats and more data to identify critical junctures. This could build on existing frameworks like the IGF PNIF's and/or ISOC's Internet Impact Assessment Toolkit
- Commit to bridging silos of internet governance discussions to better coordinate and advocate for the protection of the internet.

Civil society organisations (CSOs)

- Engage in capacity-building efforts to ensure that various parts of the internet governance community have the ability to identify and address threats to the internet.
- Identify good examples of legislation that both promotes the preservation of global connectivity and serves in the national interest of governments.
- Advocate for concrete commitments to an open, interoperable and transparent internet to be included in the upcoming ITU WTSA meeting, WSIS+20 review, NetMundial+10, and the Pact for the Future / Global Digital Compact.
- Work together to develop a report outlining the problems facing the internet, key messaging, recommendations and available tools and resources.
- Document examples of the negative impact on the open internet of certain regulation
- Collaborate with other stakeholders to support internet fragmentation measurement efforts. This could include identification of existing tools for measuring internet fragmentation, resulting gaps and ideas for addressing those gaps (e.g. to identify where the internet's 'weak points' could be/the spectrum of threats to global connectivity from policy and regulation and their impact)

Private sector

- Provide the resources and access necessary for CSOs to engage in capacity-building efforts.

- Commit to upholding the multistakeholder model of internet governance and policymaking.
- Collaborate with other stakeholders to support internet fragmentation measurement efforts

Technical community

- SDOs should commit to the preservation and strengthening of the multistakeholder approach to internet governance, including through proactive and meaningful integration of a diversity of expertise in the standard development process.
- For SDOs should raise awareness of threats arising from both policy and regulation, and from other measures, on the internet's technical layer and improve coordination to address them

Governments

- It is especially important for governments as regulators to commit to protecting the characteristics that allow the internet to interoperate and function as a network of networks.
- Commit to preserving global connectivity and ensure that policies and regulation do not interfere with what is at the core of global connectivity.
- Commit to inclusive and multistakeholder policymaking, through proactive and meaningful integration of experts. This can include the direct solicitation of expert input from across the internet governance community when developing policy/regulations that may impact the technical underpinnings of the internet.
- Adhere to human rights standards when it comes to internet governance; any restrictions on human rights standards must be consistent with the principles of legality, necessity and proportionality.
- Conduct impact assessments: governments should ensure that for any policies or pieces of legislation that have the potential to impact internet architecture, there is a review conducted to prevent unintended consequences and/or to mitigate any potential risks to the internet and its users.
- Commit to avoiding politicising the core of the internet.
- Commit to enforcing a holistic review of digital policies to ensure that all steps have been taken to prevent unintended consequences that could lead to fragmentation of the internet.