Contribution ID: d75de7b4-439b-4beb-b282-d89d7c62e654
Date: 14/01/2025 16:42:04

Targeted consultation on Internet Governance

Fields marked with * are mandatory.

Background

The European Commission is launching a targeted consultation on its stance on Internet governance in preparation for the critical milestones foreseen in 2025 (WSIS+20) and in response to the request from the Council to develop “an EU strategy on the multistakeholder governance of the Internet to set out a common position to uphold in international fora with a view to ensuring an open, free, affordable, neutral, global, interoperable, reliable and secure Internet”.

The aim is to gather input from stakeholders across governments, business, technical experts, and civil society organisations—to inform and strengthen the EU’s position. This consultation aims to refine the EU’s vision for a free, secure, and open internet while safeguarding its core values of data protection, human rights, and the rule of law in the digital space. Your insights and participation are essential to help direct the future of internet governance.

Internet governance is a system of processes, policies, and standards that shape how the internet functions and evolves. The internet is inherently decentralised, involving governments, international organisations, technical experts, businesses, and civil society organisations. The EU believes that supporting this multistakeholder approach is vital to keeping the internet free, secure, efficient, equitable, and respectful of human rights, especially in the face of rapid technological advancements.

However, the multistakeholder model of internet governance has been and is under increasing pressure in global forums, such as the recently adopted Global Digital Compact (GDC) and the upcoming World Summit on the Information Society (WSIS+20). Some governments are pushing for more centralised, state-controlled approaches, citing national

security, data privacy, and digital sovereignty concerns. While these concerns are valid, that shift risks breaking the internet into isolated national networks, undermining global connectivity, innovation, and the principles of a free, open, and accessible internet. The growing politicisation of internet standards and infrastructure—driven by market competition and geopolitical tensions between superpowers —adds to the complexity. The upcoming discussions on the future of the internet governance is an opportunity to examine the challenges and opportunities and seek solutions to ensure that it is future proof.

Against this background, the EU must clearly articulate its expectations for the outcome of WSIS+20 and make a compelling case for why a multistakeholder governance model is essential for supporting the internet's open and global nature. The EU's leadership in sustaining this model is crucial for protecting its digital interests and ensuring the global internet stays stable and open. Together with its core values—data protection, human rights, fundamental freedoms and the rule of law—the EU can secure international recognition of its digital policies and regulatory frameworks.

Privacy Statement

Before proceeding with the questionnaire please take a moment to review the privacy statement:

Targeted_consultations_privacy_notice.pdf

About you

* Full name

Patrik Fältström

* Email address

paf@netnod.se

* Which institution/organisation(s) do you represent?

Netnod

* Which stakeholder group best represents you?

Technical community

* In which country are you based?

Sweden

1. Introduction

1. According to the institution/organisation that you represent, what are the most important benefits of the open, free, global, interoperable, reliable, and secure Internet?

Maximum 3 selection(s)

- [x] a. Possibility to connect with other users worldwide
- [ ] b. Opportunity to freely express one's opinions
- [x] c. Greater access to information worldwide
- [ ] d. Greater participation to democratic processes and decision-making
- [ ] e. Greater transparency and accountability of government
- [ ] f. e-Government and cutting red tape
- [ ] g. Possibility of association
- [ ] h. Business and commercial opportunities
- [ ] i. Learning and development
- [x] j. Other

Other. Please elaborate:

Free information and dataflows architecturally separated from the network and its operation, that is, a network architecture which is not vertically integrated

2. According to the Member State/institution/organisation on whose behalf you are responding, what are the biggest threats and challenges to an open and resilient internet? Please pick your top three responses.

Maximum 3 selection(s)

- [ ] a. Cybersecurity threats targeting internet infrastructure
- [ ] b. Cybersecurity threats targeting online users
- [ ] c. Unequal access to the internet for users across the globe
- [ ] d. Disinformation and misinformation
- [ ] e. Censorship including cancelling, deplatforming, banning, etc
- [ ] f. Violation of human-rights online
- [ ] g. Insufficient privacy protection, particularly personal data
- [x] h. Rise of digital authoritarianism and state control over the internet, e.g. internet shutdowns
- [x] i. Centralised, state-centric models versus the current decentralised, multi-stakeholder structure
- [ ] j. Lack of investment in critical internet infrastructure

- [x] k. Other

Other. Please elaborate:

Current legal developments, also in the EU, such as #ChatControl and data storage directives, are incongruent with a free and open Internet where the network is technically and architecturally separated from its contents. Even well- meaning legal frameworks can have dire consequences for an open and global Internet. The ground rules for the infrastructure need to be globally congruent, and local laws (such as EU-regulation) should only concern legal entities using the Internet, not the Internet itself.

3. According to the institution/organisation that you represent, is the EU is doing enough to address the above-mentioned challenges and threats?

- ( ) Yes
- (•) No

Please pick the top three actions that you consider should be carried out.

Maximum 3 selection(s)

- [ ] a. Step up EU internal coordination with the Member States to increase its international leverage
- [ ] b. Strengthen EU action to protect the open internet on the international stage by bridging the digital divide
- [ ] c. Reinforce EU actions to protect human rights online
- [ ] d. Ensure equitable access to the Internet
- [ ] e. Promote internet freedom, counteract internet shutdowns and censorship
- [ ] f. Support the greater involvement of stakeholders from the Global South in internet governance
- [ ] g. Increase participation of EU stakeholders in the international Internet governance institutions
- [x] h. Advocate to strengthen internet governance institutions (ICANN, IETF, IGF)
- [x] i. Step up the efforts of the EU technical community in standardisation
- [ ] j. Foster internet technologies that are compliant with EU principles and norms and enable users' choice, protect their privacy, and increase their security
- [x] k. Other

Other. Please elaborate:

Ensure that all legal acts produced in the EU support an open and free Internet down to the technical level. This includes both avoiding sanctions on information exchange over the Internet, as well as updating existing legal frameworks. In other words, the EU should not do "more", rather ensure that what the EU already does is congruent with a free and open Internet.

4. According to the institution/organisation that you represent, how important is the type of governance model for an open and secure global internet (multistakeholder model versus state-centric)?

Very important

5. According to the institution/organisation that you represent, is there sufficient knowledge in the EU of the impact of internet governance on the open and secure global internet?

No

2. Coordinating and engaging EU Internet governance stakeholders

6. According to the institution/organisation that you represent, is there sufficient participation and coordination between EU stakeholders in the internet governance area?

No

7. According to the institution/organisation that you represent, how can the EU enhance participation and coordination among its internet governance stakeholders?
Please pick your preferred top three options.

Maximum 3 selection(s)

- [ ] a. Increase coordination between the national and European authorities through common positions ahead of key policy milestones
- [x] b. Create networks of technical experts to represent common EU interests in standardisation fora
- [x] c. Increase funding for national and regional initiatives, such as the national IGFs and EURODIG
- [ ] d. Increase connections between national and regional initiatives with international ones on internet governance especially the IGF
- [ ] e. Empower underrepresented groups such as youth, seniors, digital rights, and civil society organisations for active involvement in the field of Internet governance
- [x] f. Other

Other. Please specify:

Participate in existing fora, such as ICANN and IETF meetings where relevant.

8. According to the institution/organisation that you represent, what are the main barriers to effective multi-stakeholder participation in internet governance?
Please pick your preferred top three options.

Maximum 3 selection(s)

- [ ] a. Power imbalances expressed in varying interest, influence, and stake
- [ ] b. Ways of engagement that overlook the various levels of expertise, interest and influence of different stakeholder groups that vary depending on the topic
- [x] c. Technical expertise and knowledge gaps
- [x] d. Geopolitical tensions and bloc-thinking
- [ ] e. Lack of inclusivity
- [ ] f. Coordination difficulties and separate siloed discussions on specific issues risk creating incompatible and even conflicting outcomes
- [x] g. Legal and regulatory differences
- [ ] h. Resources limitations
- [ ] i. Other

3. Transforming global stakeholder organisations for inclusive, effective, and sustainable Internet governance

9. Is the institution/organisation you represent familiar with or does it participate in the work of the following Internet governance institutions/fora (pick up to 3 answers):

Maximum 3 selection(s)

- [ ] a. EURODIG
- [ ] b. Internet Governance Forum (IGF)
- [ ] c. Internet Corporation for Assigned Names and Numbers (ICANN)
- [ ] d. Internet Engineering Task Force (IETF)
- [x] e. All the above
- [ ] f. None of the above
- [ ] g. Other

10. Noting the fast-paced evolution of the internet and building on your analysis of the current IG institutions (ICANN, IETF, IGF), does the institution/organisation you represent consider that there is a need for changes or improvements to their mandates, governance, or functioning?

- (•) Yes

- ○ No
- ○ I do not know

11. If YES (to question 10) what changes/improvements would it recommend to some or all the listed Internet governance institutions?

	EURODIG	IGF	ICANN	IETF
Improve inclusivity in decision making	☐	☐	☐	☐
Review/change the internal decision making processes and institutions	☐	☐	☐	☐
Make procedures more transparent	☐	☑	☐	☐
Improve participation, including through specific support for underrepresented communities	☐	☐	☐	☐
Improve overall effectiveness/modernize the organisation	☐	☑	☐	☐
Improving effectiveness of the meetings/key events with a view to increase impact	☐	☐	☐	☐
Review the mandate to consider technology developments	☑	☑	☐	☐
Other	☑	☑	☐	☐

Other. Please specify:

Focus mission on Open Internet.

4. Emerging technologies: anticipating the governance of the future Internet

12. What are the key governance challenges associated with emerging technologies such as those underpinning Web 4.0 according to the institution /organisation you represent? Please choose your top three replies.

Maximum 3 selection(s)

- ☐ a. Uncertain definition of the scope
- ☑ b. Lack of common global standards
- ☐ c. Lack of a common institutional framework
- ☐ d. Balancing public and private interest
- ☑ f. Identifying the right balance between innovation and regulation
- ☐ g. Potential far-reaching implications for society
- ☐ h. Risk of deepening digital divide
- ☑ i. Other.

Other. Please specify:

That state actors confuse service and content made available over the Internet with the Internet itself

13. Is the institution/organisation you represent familiar with alternative (blockchain-based) domain name spaces?

- (●) Yes
- ( ) No

14. If yes, what will be their impact on the traditional DNS infrastructure and its governance (multiple answers possible) according to the institution/organisation you represent?

- [ ] a. Increased offer of domain names for consumers possibly leading to lower prices
- [ ] b. Greater freedom for internet users due to immutable and resistant to tampering nature of alternative domain names based on blockchain solutions
- [ ] c. Increased competition and innovation in the domain name space
- [ ] d. Consumer confusion linked to possible identical domain names (name collision) in the traditional DNS and in the alternative (blockchain based) DNS spaces
- [ ] e. Lower protection for intellectual property rights due to the absence of collective governance mechanisms for alternative domain name spaces
- [ ] f. Lower protection for consumers against harms due to the absence of collective governance mechanisms for alternative domain name spaces
- [x] g. Other

Other: Please specify:

None, alternate name spaces are not likely to have any impact at all at the Internet infrastructure level.

5. Internet security and resilience

15. Facing a growing number of cybersecurity threats, what does the institution /organisation you represent see as the most pressing challenges to ensure the security and resilience of the open and global Internet in the next years?

- [x] a. Possible fragmentation of the open and global Internet
- [ ] b. Insufficient deployment of advanced security features
- [x] c. Possible vulnerabilities of the global routing system

- [x] d. Availability and reliability of crucial Internet functionality in case of major incidents or in case of crisis
- [x] e. Other

16. Please briefly explain the choices above:

Fragmentation is currently a real risk, as sanctions and legal frameworks start targeting infrastructure level functions of the Internet. D) As dependence on the Internet increases for all use cases, it is likely that there are dependencies on the Internet in areas where Internet infrastructure is not built with enough robustness in mind. E) Legal frameworks working against an open, global and resilient Internet. C) Routing is not perfect, but less of an issue than previous issues.

17. According to the institution/organisation you represent, are the current policy instruments and approaches available at the EU level (coordination at EU level and cooperation with international partners, supporting EU-based critical infrastructure (such as the EU-based public DNS resolver DNS4EU) for the benefits of EU citizens and the global Internet, fostering deployment of important security standards, …) adequate with respect to these challenges?

- ○ Yes, fully adequate
- ○ Yes, partially adequate
- ◉ No

18. According to the institution/organisation you represent, how can the EU contribute better to enhance the security and resilience of its internet infrastructure and the overall Internet for the benefits of its citizens and the global Internet?

First off, policy at an EU level needs to acknowledge that policy for the Internet itself should be separate from policy for services over the Internet. The fundamental building blocks of the Internet need to be global, and globally coordinated. These building blocks include but are not limited to globally coordinated IP-address space, globally coordinated domain names, and globally accepted common protocol specifications. As long as these building blocks function the Internet will offer free flows of information for all use-cases. These building blocks are essential and are today handled in multistakeholder arenas.

Secondly, policy targeting the use of the Internet should target end-users, not the network operators. Network operators should shuffle packets to the best of their ability, not build backdoors which inevitably will be used by foreign powers to strengthen their position regarding the EU.

Thirdly, recognize that the Internet is used for essential services and systems, not only entertainment. This requires that Internet infrastructure is built in a robust and diverse manner so that single cable failures do not lead to measurable effects. For example, public procurement needs to be done in such a way that all publicly procured Internet access for important services requires redundant functions in all layers of the network (optical fibers, switching equipment, routing gear, etc).

Contact

CNECT-IG-CONSULTATION@ec.europa.eu