**IAB Response to the European Commission's exploratory consultation on "The future of the electronic communications sector and its infrastructure"**

The Internet Architecture Board (IAB) welcomes the opportunity to provide input to the European Commission's exploratory consultation on "The future of the electronic communications sector and its infrastructure". The IAB provides oversight of the architecture for protocols and procedures used by the Internet and also handles the liaison management for the Internet Engineering Task Force (IETF), the main engineering organization that works on standards relating to Internet technology.

The IETF is an open, diverse, and global community of network operators, engineers, researchers and many other stakeholders. The mission of the IETF is "to make the Internet work better" by producing "relevant technical documents that influence the way people design, use, and manage the Internet" (RFC 3935). The IETF develops, maintains and evolves the Internet protocol suite and many related standards.

In this submission we provide input to the consultation to specifically address aspects of Questions 10 and 60. Questions 53, 54 and 58 are technically not applicable, we therefore submit general comments on how the proposed changes will negatively impact the Internet Architecture and evolution of the Internet technology and standards as well as limit users in their open access to the Internet and service used on top of the Internet communication platform.

The Internet is a truly global, heterogeneous, and interconnected network of networks that can be used for communication of many different types between any interested parties connected to it. Its resilience and evolvability are due to its architectural principles, the underlying protocol suite, and the cooperation of network operators around the world. The IAB opposes policy interventions that would lead to a change in these principles, limit the ability for the Internet to evolve,

reduce the open access to the Internet, and finally induce a high risk of Internet fragmentation.

INTERNET ARCHITECTURE PRINCIPLES AND TECHNOLOGY CONSTRAINTS

The Internet Architecture is based on a set of principles that have enabled the success and growth of the Internet. The following section highlights principles that are most salient in response to the framing of this consultation.

*Sustainable and open Internet access*

Attempts to discriminate traffic based on the volume of data and services from the same origin is a violation of network neutrality. In 2021 the [Court of Justice of the EU upheld neutrality obligations of ISPs](#)[1] and deemed zero rating illegal under EU law, namely the [2015 Net Neutrality (Open Internet) Regulation](#)[2].

Moreover, attribution of the origin of traffic is difficult-to-impossible for bandwidth allocation by sources of data and services. Instead, ISPs can easily quantify the bandwidth that users consume. IP addresses, however, are foremost an instrument for traffic routing but are not meaningful in identifying traffic type or traffic origin. For example, users may request services and data through alternate networks of their choice, such as VPNs, therefore making traffic not easily attributable to specific CAPs from the perspective of the access network.

Users as well as the evolution of a diverse ecosystem of services that use the Internet communication infrastructure benefit from this separation of network access from services. Due to this separation in today's Internet the use of CDNs is ubiquitous especially but not exclusively for popular and successful content sources to the benefit of more performant and more secure services for the user. Use of CDN networks and cloud services, however, makes attribution harder  and can skew  price regulations against smaller content providers sharing the same CDNs as large content providers. In addition, discrimination of traffic will also negatively affect smaller content providers who do not use CDNs, and make it harder for new entrants to gain a foothold due to prohibitive entry costs.

Further, applying regional regulation to the global Internet and especially its payment and revenue structure risk disadvantages for users and local markets.  After the introduction of Sending Party Pays in South Korea, it was observed that content and application providers (CAPs) shifted their exchange of data offshore, thereby hurting the Internet exchange point market in the country. Increasing the length of

---

[1] https://edri.org/our-work/cjeu-in-surprise-judgment-zero-rating-is-illegal-under-eu-law/
[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32015R2120

traffic paths so that they are further away from users has a negative consequence for the environment, it costs more for telecom operators needing to connect with relevant CAPs further away and it deteriorates service quality for consumers.

*"Internetworking" must prevail*

The Internet is an interconnected network of networks. The Internet is decentralized and its layered architecture enables an unprecedented global communications system that has proven to be agile and resilient enough to handle massive traffic increases and rapid shifts in the type and direction of data flows, as was made evident during the COVID-19 pandemic. By design the network of networks facilitates the interconnection of networks to adapt without centralized management or a high level of coordination, and this flexibility provides scaling (RFC 3221) and drives innovation (RFC 4924). Adding a network to the Internet - a network of networks - requires a low barrier in order to grow Internet access and to grow new service offerings. This flexibility, growth and innovation might be put at risk with the proposed regulation by reinstating fee structures of the past where tight network control limited usages and evolution.

Conversely, the resilience of the Internet is put at risk with this proposal, because it requires heavier traffic management. Routing needs to remain lightweight and agile. Interconnection agreements are largely done via "handshake agreements" and without written contracts. The Internet's proven resilience and agility are not only supported by, but also directly due to, its open nature of interconnectivity. Lastly there is no indication that a regulation of the interconnection market is needed and the consequences will result in significant change and most likely harm to the Internet ecosystem.

*Permissionless innovation*

Technical and business plans across the globe towards digital transformation have sought to improve upon the era of telephony, however proposals aimed at "revenue sharing," "fair share," and "sender pays," appear to reinstate the termination fees of the past. If enacted, it would fundamentally undermine permissionless innovation by establishing additional barriers for new services and, ironically, slow the growth of the Internet ecosystem in Europe.

"Permissionless innovation" is a term-of-art in Internet networking that describes a layered and building-block approach to creating an Internet architecture that promotes rapid and open innovation. This principle fundamentally supports the Internet's current architecture and its continual improvement. The efficacy of this architectural design choice is affirmed by the consensus reached by regulators in the 2012 EU communications regulator report[3] that says, "both sides of the market –

---

[3]https://www.berec.europa.eu/en/document-categories/berec/others/berecs-comments-on-the-etno-proposal-for-ituwcit-or-similar-initiatives-along-these-lines

CAPs on the one hand and users of these applications on the other hand – already contribute to paying for Internet connectivity. There is no evidence that operators' network costs are already not fully covered and paid for in the Internet value chain (from CAPs at one end, to the end users, at the other)."

IMPACT ON THE USER

Identifying and managing access to the Internet beyond connectivity risks exclusion of users from the Internet and their access to content, this is a concern of access, meaningful access, and censorship.

Considering the way Internet connectivity works between endpoints (users and/or services), network traffic is not originated by the sources of data/services, but by the users who are paying subscribers to an Internet service provider and who request services and data from CAPs as determined in BEREC's preliminary assessment[4] from October 2022.  This element of user autonomy is fundamental to human rights, agency and market choice and attempts to attribute would have significant likelihood of being incorrect and would violate user privacy even if correct.

Conveying information throughout the Internet about traffic sources weakens users' privacy as it can imply the exposure of content and services requested by the user. This contradicts the improvements in technology that is core to the IETF's work in standards. Securing communication (RFC 6973) and designing an Internet that is foremost addressing the interest of the users (RFC 8890) are goals that align the mission of the IETF standards process to develop high qualitative specifications that make the Internet work better. Established IETF standards in areas such as ensuring confidentiality for Internet communications, including TLS (RFC 8446), are very widely used and see an increasing deployment. They continue to be enhanced and used in new contexts, such as with new transport protocols like QUIC (RFC 9000) or application protocols like DNS over HTTPS (RFC 8484), in order to close gaps where information leaks can impact user privacy, potentially even unintentionally, as any information connected to service usage can reveal sensitive data or metadata.

RISK OF FRAGMENTATION

Regulations that are tied to a certain **technology** limit Internet evolution and can lead to fragmentation. A network only needs to negotiate interconnection with one other network that is already connected to the rest of the global Internet. Once a network is interconnected it is reachable by anyone anywhere. The interconnection points between two networks have to interoperate but each network on the Internet can apply and deploy a different design choice based on the suite of Internet

---

[4]https://www.berec.europa.eu/en/document-categories/berec/opinions/berec-preliminary-assessment-of-the-underlying-assumptions-of-payments-from-large-caps-to-isps

protocols offered and developed by the IETF. This simple model has allowed the Internet to reach scale and continually expand. Overburdening the terms, conditions, technology or other details of these innumerable negotiations will slow Internet growth and expansion of Internet access to all people.

Regulations that are tied to a specific **jurisdiction** limit Internet evolution and can lead to fragmentation. The proponents of reinserting anything resembling the old termination fee model of the past into new regulations propose CAPs from around the globe to negotiate different arrangements under regulated conditions before they can exchange traffic with networks in Europe. This raises a high barrier for any CAP anywhere to be effectively connected to the global Internet and the consequence is a form of Internet fragmentation. Europeans will only be able to access content and services that have contracted with European ISPs. CAPs from outside Europe may no longer create content or services that Europeans can access. CAPs from inside Europe would also face additional costs and barriers to entry.

CONCLUSION

To maintain a healthy Internet ecosystem all actors need a source of revenue as well as a low entry barrier to offer new and innovative services over the Internet. This is supported and enabled by the Internet model where the network does not discriminate against the data that is transported over the network, separating Internet infrastructure and access services from Internet usage. A change in this basic principle is technically not feasible without limiting innovation which will impact users negatively in their access to new and existing services and content as well as user privacy, both in Europe and globally. Applying regulations that change these principles and therefore impact the protocol fundamentals of the Internet risks fragmentation in technology, standards, and content access.

We appeal to the European Commission to apply policy and regulations in the interest of the users. User centric policy enables open and broad access to a global Internet without risking or limiting the flexibility of the Internet architecture, nor the development and deployment of new protocols and technology, which are the foundation of innovation and the success of the Internet.

ANNOTATED REFERENCES

Alvestrand, H., "A Mission Statement for the IETF", BCP 95, RFC 3935, DOI 10.17487/RFC3935, October 2004, <https://www.rfc-editor.org/info/rfc3935>.

The goal of the IETF is to make the Internet work better. Its cardinal principles are: Open process, technical competence, volunteer core, "rough consensus and running code," and protocol ownership.

Frautschy, D., Gahnberg, C., "Old Rules in New Regulations – Why "Sender Pays" Is a Direct Threat to the Internet", May 2022, <https://www.internetsociety.org/blog/2022/05/old-rules-in-new-regulations-why-sender-pays-is-a-direct-threat-to-the-internet>.

This technical analysis by the Internet Society concludes that existing rules and newly proposed legislation in South Korea will slow the country's digital development and cause a direct threat to the Internet.

Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, DOI 10.17487/RFC6973, July 2013, <https://www.rfc-editor.org/info/rfc6973>.

This document brought privacy considerations into the IETF by aligning the needs of designers, implementers, and users of Internet protocols. It defined a thorough taxonomy and raised awareness of privacy-related design choices.