24 April 2024

GSMA-ETNO contribution to the Draft BEREC Report on the entry of large content and application providers into the markets for electronic communications networks and services

Introductory comments

The GSMA and ETNO welcome the opportunity to comment on BEREC's draft report on the entry of large content and application providers into the markets for electronic communications networks and services. BEREC's report comes at a critical time where the market for digital infrastructure as well as the formerly open internet architecture has been undergoing massive changes and the dynamics and interaction in the internet ecosystem is continuously developing with high speed. On this background it is the more important to get a profound understanding of the relationship and interaction between ECN/ECS and large content and application providers ("CAPs"); not least in view of the European Commission's ongoing work on the European connectivity challenges. From the point of view of the GSMA and ETNO there are several areas that deserve urgent attention.

The GSMA and ETNO generally find the report to be well-written and -explained with relevant examples of the relationship (collaboration, competition, and interdependence) between large CAPs and ECS/ECN operators and the report is an important contribution to establishing a common understanding of the dynamics and interactions between the players in the continuous developing internet ecosystem. Below we have provided some general and detailed comments that we believe are important aspects to consider.

We understand that BEREC's upcoming IP-IC interconnection report will also contribute importantly to a comprehensive analysis of the evolution of the internet architecture considering the technological shifts and the significance of large CAPs' own infrastructure. We hope the findings of the current report on entry of large CAPs into the market for ECS/ECN and especially its implications will be closely considered in the report on IP-IC interconnection report as both are highly intertwined and cannot be analysed separately.

Dynamics between large CAPs and ECS/ECN providers

We agree with BEREC's overall findings that large CAPs increasingly insource what was formerly purchased from traditional ECS/ECN providers thereby vertically integrating their respective online business with delivery networks; a development reflected in CAPs' increasing annual investments in infrastructure (p10).

We also agree with the fact that several of the markets where vertically integrated large CAPs continue to invest are already concentrated e.g. the market for cloud services where the three biggest players in Europe accounted for 72% in Europe in 2023 in a market that is expected to grow significantly driven by VHCN, cloudification and virtualisation of networks.

The market for voice assistants, the market for CDN and sub marine cables supporting the CAPs own businesses, online advertisement, private relay services are other markets with high concentration.

Large CAPs' proprietary caches within ISP networks, their global backbone infrastructure connecting their data centres and their proprietary content and application ecosystems are thus providing them with more control over their content delivery and strengthen their market position vis-à-vis ECS/ECN providers. As a matter of fact, large CAPs have already built not only proprietary content and application (OTT) ecosystems but are also building a "private" Internet.

In view hereof, it is essential that the regulatory framework in place does not unreasonably restrict or advantage any of the players who are active on the same relevant markets and part of the same digital ecosystem.

On this note, we agree with BEREC that it's important to carry out a robust and fact-based analysis of the whole internet ecosystem as well as the underlying infrastructure. The ongoing discussions on the future of connectivity (upcoming Digital Networks Act, which will surely include a review of the provisions, scope, and political objectives of the EECC) does indeed provide an opportunity to adapt a new telecoms framework, supported by relevant data to be collected from all market players, and the ecosystem properly assessed by competent authorities.

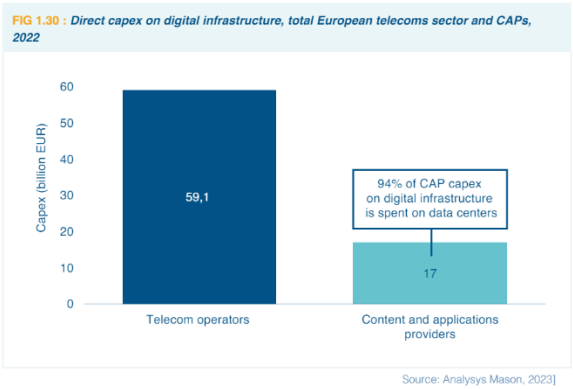
In addition to the issues identified by BEREC as potential for further investigation (impact of OS providers on ECS/ECN providers ability to give access to e.g. slicing functionalities, smaller providers' challenges in setting up some functionalities), the GSMA and ETNO believe there are more issues that could deserve further analysis. These include:

- The regulatory imbalances between CAPs and ECS/ECN providers e.g. CDN providers ability to control the user experience on top of the internet connectivity and the relationship with the Open Internet Regulation.
- The imbalance in negotiation power between CAPs and ECS/ECN providers.
- The wider implications of Internet relay services.

Overview of large CAPs investments

We welcome the presentation of detailed numbers of CAP investments in the report. It is also importantly recognised that "[…] until now CAPs have not yet invested in access networks in the EU." (p. 9) However, it would be important to show the large disproportion of the investments between

CAPs and ECNs. An illustration provided by Analysys Mason is helpful in placing the high numbers of CAP investments in perspective.



It would be also interesting to split the investment numbers into the categories “solely for private purposes” vs. “available for third parties”. In this chapter the reasons for such investments could even made clearer. Also, it would be important to dig deeper into the reasons for the deployment of own dedicated network infrastructure, as there might also be some additional incentives in addition to the better control of the provision of services in terms of improvement of quality (see remarks to case study 2: submarine cables).

For further considerations

BEREC has rightly identified the different types of dependencies (e.g., complementarity, competition, and cooperation) between CAPs and ECS/ECN providers. However, two aspects deserve attention:

Firstly, the application of the Open Internet Regulation (OIR) that influences the possibilities to compete between the ECNs and CAPs. Where Internet Access Service Providers (IASP) are subject to the strict rules of the OIR, CAPs are facing no restrictions of such kind. The OIR limits IASP’s freedom to offer services by restricting IASP`s ability to manage network traffic and offer services beyond IAS. The potential to innovate is therefore much higher at network borders than within the networks which is an unproportioned and structural disadvantage for IASP.

Secondly, the two-sidedness between CAPs and ECN providers. BEREC states that “Since no online content and applications could be consumed without connectivity, and no connectivity would be required without any online content and applications, there is an interdependence between CAPs and ECS/ECN providers.” (p. 16). It is correct, that “no online content and applications could be consumed without connectivity” as CAPs “have not yet invested in access networks in the EU” (p. 9). However, there are still services which would make connectivity necessary if large CAPs’ services were not as widespread.

Above all, if online content and applications and connectivity were actually complementary, as traffic volumes increased and services developed and diversified, then the ARPU of ECN providers would go up: the opposite, however, has been true.

Therefore, there is no meaningful complementarity.

Case study 1: Content Delivery networks

The origin of CDNs dates to the late 1990s, designed to avoid bottlenecks of internet traffic and improve the user experience. Over time, CDNs have evolved from static delivery mechanism to sophisticated platforms that can handle dynamic content, video streaming etc. Another important development is the emergence of proprietary CDNs by vertically integrated CAPs.

The CDNs capability to bringing high quality content to end-users is indisputable and underlined by the fact that in 2023 CDNs delivered more than 70% of all internet traffic worldwide and the demand is only expected to increase.

BEREC provides a good overview of the CDN market as well as the business models, but it could be helpful to explain the difference between CDNs and on-net CDNs in more detail. Further and more importantly there are a number of effects which arise from the developments in the internet ecosystem, especially the vertical integration by CAPs and its overall concentration which we encourage BEREC to take a closer look at.

Business models

Regarding business models, as noted by BEREC, there has been a significant shift in the CDN market in recent years. All major CAPs now operate their own CDNs (vertical integration) and place little reliance on the offerings of commercial CDN providers. According to WIK Consult/BNetzA (2022) the CDN business of specialised (commercial) CDN providers have thus developed less strongly than CDN traffic as a whole. The study also noted that Internet access providers and carriers have not been able to develop a successful in-house CDN business, whereas some of the large CAPs have developed their own (successful) commercial CDN business.

We welcome the well described different business models in terms of private CDNs (vertical integration by large CAPs), public CDNs (commercial CDNs), as well as mixed CDNs (vertical integration by CAPs). It is also correctly noted that the market is very concentrated, and the concentration is likely to increase in the coming years (p. 2). We would point to an area, which we believe BEREC should take a closer look at.

An important aspect of the increasing concentration of proprietary CDNs is the implications on the competitive landscape vis a vis smaller commercial CDNs (public CDNs in BEREC terms) as well as smaller CAPs.

The number of commercial CDNs has decreased over the last years with fewer players offering CDNs to third parties. This has a direct effect on the options of smaller CAPs that may face higher input costs. Also, smaller CAPs may be disadvantaged in delivering content to end users as a result of the crowding out of specialised commercial CDNs making them more dependent on large CAPs (vertically integrated CDNs). This is a development that BEREC should monitor closely as it might result in foreclosure effects by large CAPs such as self-preferencing to decrease competition. This would further cement the positions of the large CAPs and their business models based on proprietary CDNs and underline that ISPs no longer possess a gatekeeper position.

Private CDNs and cache servers are increasingly in control of the customer experience

CDNs have significant scope to shape the internet experience of end-users, as they seek to exert increasing control over the quality of experience for end-users, via solutions at a network, application, device and/or software level. Examples hereof include the expansion in the use of private networks, e.g. CDNs which are not directly covered by the open internet rules. Proprietary CDNs deployed by a non-ISP allow enhanced customer experience exclusively for the traffic delivered through that CDN, providing a competitive advantage over other content. CDN providers like Akamai can differentiate the prices and quality they offer to content providers. They can also apply traffic management techniques such as load balancing and prioritisation of traffic (e.g. in favour of live streaming) when delivering traffic.

On the contrary, rigid traffic management constraints together with restrictions on internet access services limit the possibilities of ISPs to develop competing commercial solutions. This is an important imbalance in the regulatory framework which directly effects the competitive outcome and the telecoms sector's ability to flourish, and which could lead to disintermediation of operators by digital gatekeepers and CAPs, who can provide the differentiation in services, without consideration to the principles in the Open internet regulation.

We note that the above-described practise has not given rise to any concern by regulators despite its alleged non-compliance with the principles of the open internet.

We encourage further analysis of this practise and its impact on the ECS/ECN sector and the wider internet ecosystem to ensure equal rights and obligations for all players.

In fact, CAPs possess already increasing control in several areas i) traffic level by using proprietary CDNs to allow for QoE, ii) service level by allowing only certain apps in app-stores, iii) device level by providing certain services only on certain devices, and iv) content level by interfering with unwanted content rated dangerous or simply false.

Imbalances in bargaining power

The CDN landscape as described above also contributes to increasing the imbalance in bargaining power between ECS/ECN providers and large CAPs. Large CAPs have a superior bargaining power over ISPs when it comes to negotiating fees for IP data transport which has resulted in the imbalanced ecosystem we see today. This superior bargaining power of large CAPs stems from several factors:

First, the OIR establishes the principle of Network Neutrality. Based hereon, ISPs are, in effect, subject to a "must carry" obligation of all traffic based on certain rules that are to some extend commercially and technically restricting operators from reaching optimum IP solutions.

Second, large CAPs have become indispensable for ISPs, as they provide the content and applications that end users expect from any internet service and that play a key role in their everyday lives due to their strong network effects which result in a dominant position. ISPs cannot afford to deny or degrade access to large CAPs' services, as they would face strong legal and customer reactions: ISPs are prevented by law from discriminating between types of CAPs for commercial reasons, and if an ISP denied its customers access to Netflix or Facebook, it is more likely that its customers would

switch to another ISP than that they use another content. Thus, those players can make use of their dominant position in their core revenue generating markets.

Third, large CAPs are less dependent on large ISPs, as they have alternative options (routes) to reach their end users via other networks, such as commercial CDNs, cloud operators, or other carriers. These networks are interconnected to the ISPs' networks through existing peering and transit agreements, which enable the free flow of traffic between different networks in line with the OIR. Therefore, large CAPs do not need to obtain direct connectivity from a particular ISP to access its customers even if for the detriment of CAPs' customers; in fact, CAPs have adopted traffic routing decision detrimental to their customers with the purpose to pressure network operators as publicly responsible worsened customers' experiences thereby exhibiting a clear sign of a strong market dominant position. A vertically integrated ISP is not able to withhold access to its infrastructure, as it applies the principle of network neutrality and must deliver any traffic that enters its network to end users on a non-discriminatory basis. As a result, even without a direct commercial agreement with a carrier, a CAP is still able to reach its end users via indirect connections and/or CDNs and/or cloud operators.

Fourth, large CAPs have a significant quality lever over ISPs, as they can influence the quality of service and network stability of ISPs by their own routing decisions. Large CAPs, which send particularly large volumes of data, can congest specific interconnection points by spontaneously re-routing a portion of their traffic via indirect connections to the ISP's network, thereby affecting the quality of service for all online services routed via the affected interconnects. This can induce a quality-adjusted price increase for end users on the ISP's network, which would deteriorate the ISP's competitive position if the CAP leaves connections to other ISPs unaffected.

Fifth, end users tend to hold ISPs responsible for any quality problems, even if caused by the CAP, and are more likely to switch their ISP than to stop using the CAP's services in case of persistent connection issues. Large CAPs can impact the quality of services of a network carrier with an integrated ISP business towards its end customers, which is a central dimension of competition at retail level, and evidence shows that in case of any connection problem, end users react negatively towards their ISP and not the CAP. This effect is exacerbated by the fact that certain CAPs display to internet users ISPs ranking according to the quality level of the provision of their own service(s) with respect to CAPs' chosen criterion, effectively steering end-users to their preferred ISP. This is thus a powerful mechanism that can be used in negotiation between large CAPs and ISPs.

The benefits of CDNs for ECN operators are not significant

As pointed out by BEREC, ISPs may be interconnected with CDN providers via peering agreements, or ISPs may host CDN servers in their networks. The latter approach bring content as close to the end user as possible and ensure high quality content to the benefit of end users. BEREC suggest that ISP hosting CDN services may also be motivated by reduced capacity costs (peering interconnection, backbone and backhaul links (p. 29).

While CDNs may have a positive impact on improving the quality of content to the end users, the view of GSMA and ETNO is that their impact on capacity cost and thus network investment requirement for delivering the traffic from CAPs is limited.

The cost savings resulting from CDNs and on-net CDNs (i.e. cost saving related to international transport and operators' national backbone) are not significant when compared to the total and

traffic related networks costs, considering that CDN investment has very limited bearing on the volume of traffic on the access network.

It should be noted that CAPs normally provide and maintain the cache servers (on-net CDNs), but ECNs bear the set-up costs and operational costs, which further limits the benefits. For mobile networks the use of on-net CDNs is even less viable as the international transport cost saving is relatively lower when compared to total network costs, as access networks bear the highest share. CDNs do not reduce bandwidth requirements for mobile access networks since cache servers must be located upstream where mobile traffic is aggregated.

Finally, CDNs leads to less control for ECS/ECN providers over their own infrastructure, thus increasing dependence on CAPs.

Additional general comments

BEREC states "This duality, in which some CDN providers act as applications on top of the internet, while others have their own infrastructure and therefore do not need to acquire connectivity from an ISP, was highlighted in the BEREC Report "An assessment of IP interconnection in the context of Net Neutrality." (p. 23) We would like to highlight that connectivity does not only mean the "interconnect" but also includes the connectivity to the end-user. Thus, "do not need to acquire connectivity from an ISP" does not provide the full picture.

Throughout the report, BEREC use the term "termination of traffic to the end-users" e.g. "CAPs may buy transport services from operators. If CAPs operate their own CDNs, they are less reliant on transit services, but still need telecommunications operators for the "termination of the traffic" to the end-users". From the point of view of the GSMA and ETNO, "delivery of the traffic" is a more correct term to use which describes the actual service provided by the ISPs.

Case study 2: Submarine cables

BEREC has correctly highlighted that "the international submarine cable connectivity market has witnessed significant changes, particularly with the involvement of large CAPs" (p. 31). There are two points we would like to highlight.

First, it would be important to better understand the reasons for the deployment of own submarine cables, as there might be additional incentives in addition to the better control of the provision of services in terms of improvement of quality.

Considering investments in submarine cables, and despite ample capacity at peak supply in a typical pork cycle, large CAPs continue to invest heavily in subsea cables notably on the routes connecting Europe with the US. CAPs benefit from deep pockets, facilitating strategic investments in critical infrastructure without the need for an adequate return. Given that cheap trans-Atlantic capacity is generally available means that the intention of large CAPs could be to acquire "control" over the Internet. In fact, Google, Meta and other large CAPs are quietly buying up the most important part of the Internet. Historically, subsea-cables were owned by various groups of private companies — mostly regulated telecom providers. A situation which has changed; The year 2016 saw the start of a massive submarine cable boom, with buyers being content providers — corporations like Google,

Meta, Amazon, and Microsoft. Amazon and Microsoft now part-own one and four networks, respectively.

By routing traffic through their own infrastructures, large CAPs can bypass the public Internet, thereby strategically reducing or eliminating their reliance on best-effort Internet. The increasing circumvention of the traditional Internet architecture of Tier-1 and Tier-2 networks is referred to as "Internet flattening". These unregulated infrastructure investments are the reason why the formerly decentralised architecture of the Internet has become increasingly centralised towards a few large CAPs and represent a significant change compared to the original aim of the open Internet to globally connect all users for the benefit of society at large.

Second, BEREC states that “Large CAPs predominantly use the capacity on the submarine cables for their own internal needs, particularly for interconnecting their data centres” (p. 33). As a result, those investments mostly do not provide any additional competitive or resilience component as BEREC correctly states: “In this context, while large CAPs deploy submarine cables primary for their own use, traditional ECS/ECN providers still play a key role on the transmission of data for other CAPs, connecting areas which may not be economically profitable. Therefore, by primarily interconnecting their data centres and regional PoPs to data centres, large CAPs’ investments have limited impact on the global network resilience.” (p. 54)

As ECS/ECN providers are forced into routes which are “not economically profitable” there is a further imbalance between CAPs and ECNs which also makes Europe more reliant on the large CAPs, thus reducing its sovereignty.

Case study 3: Internet relay services

The protection of privacy and personal data is an important and recognised objective. However, private relay solutions tend to go beyond what is necessary and lead to a number of undesirable effects in areas that are also important and worthy of protection. As a result of respective encryption and the masking of IP-Addresses, the affected traffic will no longer be identifiable, even to providers of Internet access services. This has not only a negative impact on the established business models of these providers, but also leads to restrictions on competition and innovation and a further undesirable concentration of traffic on the Internet in the hands of a few powerful Internet companies[1]. Above all, it also jeopardises the security and resilience of communication networks. Overall, this undermines the desired European sovereignty in digitalisation.

We partly agree with BEREC’s analysis of the potential impact of private relay services on operator networks (fixed, mobile etc.) and we believe more analysis is needed. Internet relay services are not a VPN and need to be distinguished from them. Also there exist several flavours of relay services (e. g. Apple iCloud Relay, Microsoft Edge Secure Network and Google IP Protection), although, always with the same CAPs in the background (e.g. Cloudflare, Akamai, Fastly). VPNs are mainly used within business environments or by experts, i.e. by a small portion of all Internet users. With Internet relay services, almost 100% of the Internet traffic might be processed by only a few CAPs, which contradicts all the basics of the decentralised Internet that we know today. Below we have

[1] Draft BEREC BoR (24) 51, no. 6.4.4., p. 47.

highlighted issues of particular importance for network operators and encourage BEREC to further investigate the undesired impact of these services.

Traffic management is strongly impacted by Internet relay services. ISPs optimise their networks to provide the best user experience, i.e. high data rates and very low latency as shown in Figure 1. By national law, ISPs are obliged to block illegal content or to offer specific services free of charge. Additionally, ISP filter malicious content to protect their customers from malware and phishing attacks.

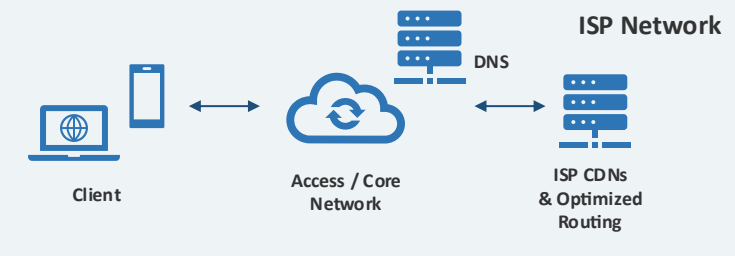


Figure 1: Without Internet Relay Services

Internet relay services bypass the carrier Domain Name System (DNS) server, and thus the optimised ISP network, resulting in substantial limitations and implications for customers, enterprises, and authorities, etc. as shown in Figure 2.

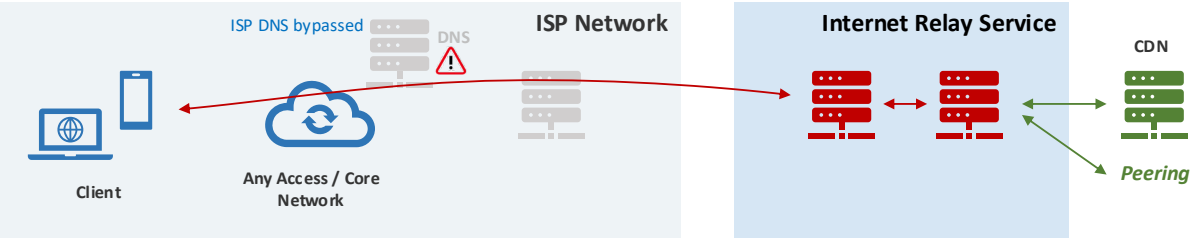


Figure 2: With Internet Relay Services

As Internet relay services are currently not considered a publicly electronic communication service, there is no requirement to notify the service to regulatory authorities (subject to local law). Internet relay services would thus not comply with the measures under European law such as e.g., the directive on Network and Security Systems, legal interception measures, and privacy legislation. Currently competent authorities of the Member States are not able to intercept Internet traffic because of the lack of obligations on the part of the relay provider to enable lawful interception.

From the perspective of network operators, a main concern is that the significance of Internet relay services (private proxy relays) has the potential to develop from affecting a minor portion of traffic into potentially being the mainstream default. Besides, the introduction of Internet relay services yields a strong potential for centralisation of the Internet. During the last year, 97% of internet traffic

in the EU[2] was generated by devices with operating systems from Apple, Google and Microsoft as shown in Figure 3.

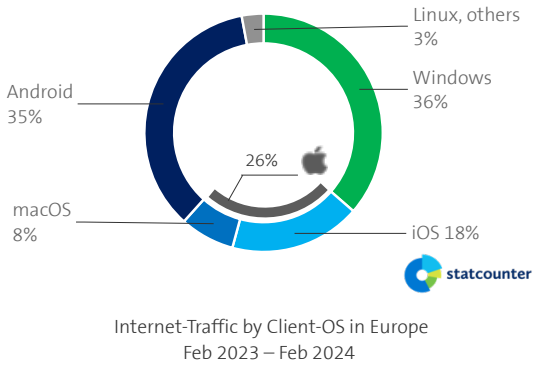


Figure 3: Internet traffic in EU by client operating system

The corresponding Internet relay services are also in the hands of these three companies, however usually in collaboration with at least one of three large (US-based) companies Cloudflare, Akamai and Fastly. CAPs therefore have potential for completely controlling the Internet traffic initiated by end-user devices in Europe. By taking over the important control point DNS (which is an essential part of the Internet Relay Service), CAPs could then be in control over many other Internet services as well. At the same time, existing offers, and services from European companies (incl. ISPs) could be impacted; both services provided for free and against a fee.

It should be noted that many of the mentioned implications are not only caused by Internet relay services but also by other services, introduced by CAPs, such as e.g. DNS encryption (e. g. DNS-over-TLS, DNS-over-HTTPs, oblivious DNS-over-HTTPs) and/or encrypted network protocols (e.g. QUIC), that cannot be intercepted.

Below we highlight some of the implications of Internet relay services that are of high concern to network operators (ISPs):

1. Products and Services are affected

- ISPs must implement workarounds to ensure that certain products and services can continue to function. These workarounds come at a cost to ISPs.
- Some services, e.g., security services for B2B customers, blocking of web pages malware or phishing, parental control, filtering of adult content for minors, can no longer be offered because no workarounds exist as Internet Relay Service implementations have made them impossible.
- Relay services take away a substantial amount of new and existing business opportunities from ISPs, and services based on 5G enabled network slicing may eventually be affected.
- The OS messages shown on end-user devices regarding Internet relay services bring ISPs and their network-integrated services into disrepute.

[2] https://gs.statcounter.com/os-market-share/all/europe

- Unfair advertising for Internet relay services included in (error) messages in the client operating system distorts competition.
- Default encrypted DNS resolvers in Internet relay services or in Internet browsers (e. g. Firefox) bypass DNS resolvers form ISPs.

2. Omission of DNS

- Security functions based on DNS, such as identifying websites that spread malware or phishing websites, can no longer be offered.
- Other services, especially in the security environment, e.g., blocking web pages with malicious content, data loss prevention (DLP), and any other DNS-based security solutions can no longer be offered.

3. Customer support becomes more complex and expensive.

- Internet relays service implementations make a range of services impossible, including those from third parties. For customers, the root cause of failures or malfunctions of Internet services is rarely traceable and most customers turn first to their ISP. In the case of errors or failures of an Internet relay service, customers will first contact their ISP because it looks to them as if the Internet access is not working. The ISP is then faced with support effort even though its own services are not affected and are not the root cause.
- Customer perception and satisfaction deteriorates, and new costs are incurred for ISPs due to higher customer care volumes.
- Customers may be frustrated as they would usually not understand the technical implications and the trust in European ISPs would decrease.

4. Customers must be informed

- ISPs have little choice but to inform customers reactively and/or proactively. This is time-consuming and causes costs.
- Unfortunately, it must be assumed that not all customers and media will perceive this information positively, as misunderstandings can foreseeably arise. It could result in an "ISP against Apple" or "ISP against the privacy of their customers" among consumers that is not encouraging for any of the parties.

5. Implications for residential customers of ISPs

- **Lawful Interception by the USA**
  Through the Cloud Act, Internet relay services enable American authorities to demand (and combine relay) data on European citizens or residents or visitors to Europe directly from Apple, Google, Microsoft or their partners, without the need for a European court to approve this or for those affected to be informed.

- **Performance Losses**
  By adding several additional systems (aka hubs), both the latency and the speed are affected

with every Internet access. Especially the increase of latency has a noticeable negative effect in practice.

- **Choice Limitations for Services & Products**
  With the introduction of Internet relay service implementations, the use of certain products and services from ISPs is possible only if the customer switches them off. This for example concerns security solutions built into the network that prevent access to dangerous sites (malware, phishing, etc.) or enable "parental control". However, the users are usually advised against deactivating Internet relay services directly in the user interface of the operating system and as a result, residential customers will primarily switch to services and products provided by Apple, Microsoft, Google or their partners. The freedom of choice is therefore somehow jeopardized, and in some cases, completely restricted.

- **Misleading and unfair Advertising**
  Customers are misled by Internet relay service provider (error) messages on the end-user devices. They are led to believe that European ISPs or their services are not trustworthy and are implicitly confronted with potentially unwanted advertising for CAP services, which consumers often cannot recognise as such.

- **Loss of Quality and Stability**
  Internet relay services and similar centralised services have the potential to degrade the performance of many Internet services (especially local ones). Much of this is the direct consequence of the implications for ISPs as described above. Of course, this also has a direct impact on customers.

- **Real Privacy**
  Non-European CAPs will have far more user data available than today for any analyses. The advertised privacy by Internet relay services is provided only if no entity operates both ingress and egress server if there is no collusion between both operators and if no national authority (e. g. US authorities) can access all data. There exists no public information on the fulfillment of these requirements, but measurements show that at least one CAP has operated both ingress and egress server in the same AS (autonomous system) for one Internet relay service[3].

6. Implications for business customers of ISPs

- **Cyber Security Measures will be obsolete**
  According to Eurostat[4], there are about 22 million companies in the European Union. From many SOHOs and SMEs up to well-known large international corporations. Most of these companies have of course taken measures to increase their security in the cyberspace.

[3] https://dl.acm.org/doi/pdf/10.1145/3517745.3561426

[4] Eurostat (statistics explained), November 2023

Without active intervention by the companies, Internet relay service implementations will render these measures partially or sometimes even completely useless.

- **Further Implications**
  Many of the implications listed above for residential customers and ISPs can also directly or indirectly affect business customers. For example, their own digital products and services may no longer function in part or as a whole. Possible losses in performance, quality or stability can also have a damaging effect on business customers. For a European SME it may be difficult to set up a dialogue with a large CAP in case of any (potential blocking) issues.

7. Implications for Society

- **Lawful Interception**
  In the context of law enforcement, ISPs can no longer answer queries about users' browsing behavior when Internet relay services are switched on. The local authorities in Europe must turn to Apple, Microsoft and Google and its partners.
- **Enforcement of European regulation**
  With the limitations described above, lawful interception and content filtering must be provided via foreign companies. Compliance with European regulations and laws could be difficult or sometimes even impossible to be enforced by local authorities.

- **Content Blocking**
  The blocking of unwanted or unauthorised content such as child pornography or copyright infringements can (in part) only be implemented via Internet service relay partners and/or its peering partners. As of now, the corresponding mechanisms provided by national ISPs for decades are being undermined by Internet relay services.

Systemic Cluster Risk

Over the last months we've seen many of the CAPs faced with major outages (e. g. AWS[5], Facebook[6] and Apple[7]). The large radius of those events poses a risk and may have negative economic and social implications.[8] The APARNET[9] (the blueprint of the modern Internet[10]) was designed to be decentralised and hence highly resilient. The increasing centralisation could put the resilience of the internet at risk.

[5] https://techcrunch.com/2021/12/22/aws-just-cant-catch-a-break/
[6] https://appleinsider.com/articles/21/10/04/facebook-says-faulty-configuration-change-to-blame-for-6-hour-outage
[7] https://www.theverge.com/2022/3/22/22991792/apple-music-app-store-is-down-outage
[8] https://techcrunch.com/2021/12/22/aws-just-cant-catch-a-break/
[9] The ARPANET and Computer Networks
[10] The History of the Internet: the Missing Narratives

Oligopoly vs. Self-Determination

The introduction of Internet relay services is all ostensibly aimed at a justified goal – privacy and data protection for users on the Internet. However, the centralised implementation by the device, operating system or Internet browser manufacturers causes a potential accompanying oligopolisation of Internet traffic. This is intensified by the already existing concentration of the cloud market. The acceleration of relay services could thus have an impact on the digital self-determination of Europe and its citizens, as well as on the innovation and competitiveness of Europe as a digital and non-digital marketplace.

Conclusion

European Policy makers and individual Member States must consider whether this "loss of sovereignty" is acceptable. Creating online anonymity by Internet relay services by the CAPs, may have implications for Europe's open society and way of life. The impacts could be vast and manifold, as highlighted above.

Restrictions on access to services or functionalities by OS providers

As highlighted by BEREC, recent technological developments have led to a situation where Operating System (OS) providers increasingly are in control of access to services and functionalities.

As a matter of fact, OS providers are another group of players in the internet ecosystem that are not constrained by compliance with the current Open Internet regulation: instead, they are able to exploit it, whilst at the same time foreclosing the capability of network operators to offer differentiation-based services and business models widely adopted by CAPs or operating systems providers.

OS & slicing

Operating systems have developed so they can 'open up' end-user devices to network slices.

For example, it is now possible to split the applications on a device between 'work' and 'personal' and deliver the 'work' applications over a specific slice, optimised for that content. However, the operating systems are, for now, maintaining sole control over the designation of applications and the mapping of applications to dedicated slices.

In this respect it could be relevant for BEREC to further assess whether and how to incentivise or mandate the OS to systematically share information with mobile network operators.