Contribution ID: 46341b8a-9df0-453c-9fdc-d8964deb7975
Date: 24/04/2024 17:11:28

Public consultation on the draft BEREC Report on the entry of large content and application providers into the markets for electronic communications networks and services

Fields marked with * are mandatory.

General information

During the 58th BEREC plenary meeting (7 March 2024), the Board of Regulators has approved the draft BEREC Report on the entry of large content and application providers into the markets for electronic communications networks and services for public consultation.
This report gives an overview of the impact of large CAPs on the markets for ECN and ECS in Europe, by presenting their strategies, business models, and relations with traditional ECN/ECS providers in terms of competition, cooperation and interdependence.
In order to better analyse the implications of the CAPs' presence and strategies in ECS/ECN markets, three case studies focusing on CDNs, submarine cables and internet relay services, are carried out. Moreover, the report also highlights some potential restrictions that may be imposed by operating systems providers on ECN/ECS operators.

Your details

* First Name and Surname

Petra Arts

* Email

[redacted]@cloudflare.com

* Organisation name (in case you are replying on behalf of your organisation)

Cloudflare

* Country of origin

United States

Language of your contribution

English

Practical details of the public consultation

Stakeholders are invited to comment and provide their views on the different chapters of the draft report following its structure:

Executive summary
Chapter 1 - Introduction
Chapter 2 - Overview of large CAPs investments
Chapter 3 - Dynamics between large CAPs and ECS/ECN operators
Chapter 4 - Case study 1: Content delivery networks
Chapter 5 - Case study 2: Submarine cables
Chapter 6 - Case study 3: Internet relay services
Chapter 7 - Restrictions on access to services or functionalities by OS providers
Chapter 8 - Conclusions
Chapter 9 - Future work

Stakeholders may also upload a document as a part of their contribution, see below.

In order to facilitate the processing of the responses, the comments provided should clearly refer to certain sections/subsections/paragraphs of the draft report.

Stakeholders may submit their contributions by **24 April 2024 close of business**.

In accordance with the BEREC policy on public consultations, BEREC will publish all contributions and a summary of the contributions, respecting confidentiality requests. Any such requests should clearly indicate which information is considered confidential and be accompanied by a non-confidential version.

Public consultation

Please indicate comments on Executive summary and Chapter 1- Introduction

5000 character(s) maximum

BEREC has an important role to play in describing the current state of the EU's market for telecommunication and content services. We are concerned, however, that the draft report does not accurately describe the way different companies -- many of which offer a huge range of services -- currently operate in the market, nor does it reflect an understanding of a vision for the networks of the future. In order to fulfil the need for a vast array of digital services that consumers and businesses will demand in the future, networks will have to adjust, providing compute capacity closer to end-users. A huge range of businesses, including traditional ECN/ECS operators, are currently moving into the space to help meet the anticipated demand.

As an example of the concern, throughout the report, BEREC uses the term "CAP" to describe companies providing a wide range of different services, including services also offered by ECS/ECN operators (e.g. CDN or cloud services offered by a traditional large telecom provider). To accurately describe the market, BEREC cannot suggest that a particular company offering a wide range of services can adequately be described in a catch all category like "CAP" or "ECN" for all of the services it offers. Cloudflare recommends that BEREC reconsider its arbitrary grouping of a variety of different companies that offer a significant range of different services, and instead focus its comments on the markets for specific services being offered.

We would also like to call specific attention to the difference between the catchall terms "CAP" and "CDN", which helps demonstrate why BEREC's use of the term "CAP" does not accurately reflect the architecture of the Internet. According to BEREC's own definition, "a CAP is a company which makes content (e.g. webpages, blogs or videos) and/or applications (e.g. search engines, Voice over Internet Protocol (VoIP) and /or services available on the internet." (1) By contrast, a CDN is a mechanism for protecting and speeding up the delivery of the Content and Application Providers' traffic. Grouping CDN services and CAP services together as one category creates confusion throughout the report because of the complementary but distinct roles of the two services.

For example, the draft report attempts to distinguish CAPs and other service providers such as commercial CDN providers in some parts (for example on page 2 it is stated that "previously, large CAPs relied on commercial CDNs providers for their services, but in recent years they have been increasingly rolling out their own CDN infrastructure networks"), but in other cases, such as on page 5 and 6, the draft report groups together a number of companies that provide vastly different services and qualifies them all as "major CAPs". The term "large" and "major" CAPs are also used interchangeably, which leads to further confusion.

In this regard, we also recommend that BEREC refrain from grouping the companies that participated in the survey together into one category - for example calling them "nine major CAPs" (page 5) - as they provide a vast array of very different types of services. A description such as "the companies surveyed" would be more appropriate throughout the report.

(1) https://www.berec.europa.eu/en/open-internet/scope

Please indicate comments on Chapter 2 - Overview of large CAPs investments

5000 character(s) maximum

Please indicate comments on Chapter 3 - Dynamics between large CAPs and ECS/ECN operators

5000 character(s) maximum

We agree with the statement in the first paragraph in section 3.1 about the complementary services offered by "CAPs" and ECS/ECN operators. Specifically, this statement captures, in Cloudflare's view, the vast majority of the relationship: "ECS/ECN operators typically provide connectivity, while CAPs provide content and applications, and may provide other elements in the Internet value chain, such as operating systems (OS), app stores and devices". While the report correctly notes that other areas of competition and cooperation do exist, they are tiny in comparison to the dominant force which is the complementary aspect of ECS/ECN and "CAP" services.

We'd also like to call attention to the difference between "CAPs" and CDNs, and suggest that they play different roles in the architecture of the Internet. According to BEREC's own definition, "a CAP is a company which makes content (e.g. webpages, blogs or videos) and/or applications (e.g. search engines, Voice over Internet Protocol (VoIP) and/or services available on the internet." (1) By contrast, a CDN is a mechanism for protecting and speeding up the delivery of the Content and Application Providers' traffic. BEREC should therefore not group CDNs and CAPs together as one category, as it creates confusion throughout the report about what types of services BEREC is attempting to reference. Similarly, references like "CAPs are the main customers of a CDN provider" (page 22) are contributing to this confusion. BEREC's analysis should rather be based on the types of services that are provided, regardless of whether these are provided by a "CAP", a CDN provider, an ECS/ECN provider or others.

(1) https://www.berec.europa.eu/en/open-internet/scope

Please indicate comments on Chapter 4 - Case study 1: Content delivery networks

5000 character(s) maximum

We do not agree with some of the characterisations about the CDN market in this section. We would object to the conclusion reached by the draft report that the CDN market is concentrated, after first noting that "the CDN market may be segmented based on several criteria" and that "it is not straightforward to obtain CDNs' market shares as they vary between sources and according to whether they are measured on a traffic, customers or revenue basis". It seems that the different sources quoted by BEREC in the draft report are not giving a conclusive picture or clear evidence about concentration, and that such a conclusion is therefore premature.

For example, regarding the data points presented on page 27 based on the Web Almanac source, the draft report fails to mention that, according to the same data source, 71% of HTML requests hit the origin directly without using a CDN. Using the breakdown of CDN providers, only 15% of website requests would be served from Cloudflare.

Additionally, the cited methodology weights every website equally, and makes no adjustments for amount of traffic or website "hits". As examples, Google.com, netflix.com, and youtube.com are likely each counted as 1 website in this methodology.The draft report appears to list four different data sources for the size of CDNs relative to each other. It appears that in two of those sources, Cloudflare is the biggest. In the other two, Akamai leads, followed by Amazon, then Cloudflare. As an additional data point, Cloudflare is not listed in the top 20 sources of data entering ISP networks in France, according to ARCEP (1).

No matter which metric is used, Cloudflare's free plan (which includes DDoS protection and CDN services) is likely a significant contributor. Anyone – small business owners, individuals – can set up a website on any hosting provider and protect it with Cloudflare's free plan in a matter of minutes.

We also observe that, regardless of the conclusion reached about concentration, the CDN market is

incredibly competitive. Since CDNs sit “in front” of origin servers, website owners can easily swap out CDNs. Increasingly, we see large customers use a “multi-CDN” approach, bidding CDNs against each other to find the lowest price. After all, it’s trivial for a CAP to have two URLs, cdn1.gameprovider.com/bigfile.iso and cdn2.gameprovider.com/bigfile.iso, and simply change which URL is used.

We would also like to comment on the ways in which CDNs interconnect with Internet Service Providers (ISPs). As the WIK report states, “For large ISPs that do not allow on-net caching, on the other hand, little has changed in the classic model of the two-sided market.”(2) It is true that little has changed – how CDNs reach large ISPs is a critical part in understanding CDNs. However, CDNs and large ISPs don’t operate in a two-sided market. A two-sided market needs many buyers and many sellers. When an end-user requests content from a CDN, the CDN has to find a way to reach the user’s ISP. There is a single seller for capacity to reach that end user. This dynamic allows ISPs to charge for peering, and reduces interconnection and performance for consumers.

According to the latest ARCEP report, peering and transit make up the same share of traffic in 2021 in France as they did in 2020. On-net caches are also essentially flat, and actually went down from 21% to 17% as a percentage of traffic between 2020 and 2021. In our experience, the largest ISPs remain reluctant to allow on-net caches despite the performance gains they provide their customers.

Moreover, if a CDN is the network which delivers content and services from a content or application provider to the ISP (including, as mentioned in the draft report, in the case of a large CAP providing a mixed-use CDN - page 30), it does not seem possible that 50% of Google’s traffic does not use its own CDN. It appears that the WIK report referenced is suggesting that 50% of Google’s traffic comes from on-net caches.

(1) https://en.arcep.fr/uploads/tx_gspublication/report-state-internet-2022-300622.pdf, page 42
(2) https://www.bundesnetzagentur.de/EN/Areas/Telecommunications/Companies/Digitisation/Peering/download.p%20df?__blob=publicationFile&v=1 page XIV, para 37.

Please indicate comments on Chapter 5 - Case study 2: Submarine cables

5000 character(s) maximum

While we share and appreciate BEREC's attention to connectivity and competition in Europe, we think the conclusion of this chapter, that increased involvement in submarine cables by large companies "has profound implications for connectivity, competition, and infrastructure investment within the sector" (page 38) overstates the changes and their impact on connectivity.

One way to understand the changes in submarine cable ownership is to think about it in relation to expansion of CDNs and the local delivery of traffic. As the use of CDNs has grown, Internet traffic has localised: for cachable content, it is common for Internet Service Providers (ISPs) to interconnect with CDNs in the local market or country of their user, which means content is also served locally.

Only when the CDN does not have a copy of a file in its cache does it need to fetch that content from an origin server. Here as well, origin servers have been localising. It is now common for large content and application service providers to have multiple "cloud regions" on every major continent. For cacheable content, only when the origin is across an ocean or sea does the CDN need to use submarine capacity for that traffic. For these reasons, it seems implausible that "most internet traffic traverse international submarine cables" (page 39); however it is plausible that most international Internet traffic, or inter-regional Internet traffic, traverses submarine cables.

Following from this example, and as the draft report correctly points out, one of the most common needs for submarine capacity now is non-cacheable cloud-to-cloud traffic. This might be, for example, backups of data, logging, synchronisation to move data closer to end-users, or real time communication.
It seems only natural that as large content and application service providers have needed more capacity to send data from themselves, to themselves, they've sought to expand total inter-regional capacity while getting ownership economics for those transmissions instead of renter economics.

The draft report says there is a shortage of submarine cables between the EU and Latin America, and that such a shortage adds to costs, and increases "risk associated with data sovereignty for both EU and Latin America". Of course, having less capacity means higher prices. So to the extent there is limited capacity on those routes, those higher costs will be borne by the networks using that capacity, which are often large content and application service providers. It is unclear what is meant by "risks to data sovereignty" (page 39) and we would ask BEREC to clarify this point further.

The draft report also doesn't acknowledge that large service providers continue to develop both new submarine system routes, as well as additional capacity on existing routes, such as SeaMeWe-6 (with development from Orange), Amitie (with development from Orange and Vodafone), MAREA (with development from Telxius), 2Africa (with development from Orange and Vodafone), Blue (with development from Sparkle). These developments continue where there is acceptable business opportunity to invest.

Please indicate comments on Chapter 6 - Case study 3: Internet relay services

5000 character(s) maximum

Internet relay services are an important and continually developing privacy-preserving technology. The Internet was not originally built with security or privacy in mind, and was not meant to accommodate the privacy that end-users - and many governments and regulators - expect today. Internet relay services are a way of building that privacy in. Users have the option of using the technology with their Internet connection, and the services operate on the open Internet. To the extent that they prevent Internet Service Providers (ISPs) from inspecting traffic flows and disrupt a “business model [which] rel[y] on users’ data monetisation” (page 47), that is a feature, not a bug. Regulators who are concerned about ensuring the online privacy of European end-users should be encouraging technological privacy enhancements, not discouraging them.

As the draft report notes, using an “over the top” service to enhance privacy is not new, even if the methods are changing and improving. Specifically “Virtual Private Networks” have long been used by consumers to encrypt and proxy their traffic through a third party network. When used in this manner, a “VPN” is not serving as a “private network”, rather it is serving as a proxy or relay. The introduction to Chapter 6 of the draft report has the potential to create confusion between a VPN used by an enterprise to allow remote employees to access resources, and the use of a VPN by consumers to proxy their traffic.

We would also like to comment on the impact of relay services on interconnection. The most important factor in understanding the relationship between any digital service provider and any ISP is the termination monopoly that ISPs hold over their users. Regardless of which service delivers traffic to the ISP – and regardless of whether that traffic was proxied – the ISP still controls how much capacity they give to any other network.

The draft report gives the impression that all the interconnection happens between the ISP and the provider of the relay service. Already, it is possible that another network provides the “relay #1” service on behalf of the provider that is offering the relay service to users. Over time, we expect many networks will have the capability to provide these services.

Lastly, the draft report indexes highly on one implementation of a privacy-preserving Internet relay from one company. While this is a great offering, there are other implementations of privacy relays. For example, Cloudflare works with a leading female health app that wanted to enable an “anonymous mode” where they didn’t have access to their users’ IP addresses, and Cloudflare wouldn’t have access to their user data. We were able to achieve this using Cloudflare’s Privacy Gateway (1). Whether the desire for privacy comes from the app or the client, these privacy proxies are good for users, and good for the Internet.

(1) https://blog.cloudflare.com/building-privacy-into-internet-standards-and-how-to-make-your-app-more-private-today

Please indicate comments on Chapter 7 - Restrictions on access to services or functionalities by OS providers

5000 character(s) maximum

Please indicate comments on Chapter 8 - Conclusions

5000 character(s) maximum

Please indicate comments on Chapter 9 - Future work

5000 character(s) maximum

Please upload your file (max file size is 1MB)

Please specify which part of your response should be treated as confidential, if any.

5000 character(s) maximum

THANK YOU FOR YOUR CONTRIBUTION

Contact

Kristina.BALKIENE@berec.europa.eu