Public Cloud Infrastructure Services Market Investigation

February 2025

I. Introduction

We welcome the opportunity to submit our views to the CMA in response to its recently published Provisional Decision Report (PDR) further to its ongoing Cloud Market Investigation. We share the CMA's overall view that competition in cloud services across the UK is not working well. We believe that, as a result of ineffective competition, there is also more potential for cloud services to drive better security and efficiency outcomes. Although the CMA's latest findings are a step in the right direction there is more to do in ensuring that all businesses and end-customers can benefit from the transition to the cloud on an equal footing.

Cloudflare is a connectivity cloud provider that supplies solutions empowering organizations to make their employees, applications and networks faster, more resilient and more secure everywhere, while reducing complexity and cost.[1] Cloudflare's suite of services includes 1) services that secure and deliver content, data and applications; 2) a serverless computing developer platform, which includes products for edge-hosted code, data storage, and Artificial Intelligence models, and 3) Zero Trust security products, which offer customer employees the ability to authenticate and securely connect to internal resources from anywhere.

This submission sets out Cloudflare's views on the cloud computing market as well as on potential regulatory intervention remedies that could be explored.

II. Background

'Cloud computing' is often understood to mean providers offering store and compute. However, it can also refer to a wide variety of software and infrastructure services that are accessed over the Internet. Although the CMA breaks down this model into Infrastructure as a Service (IaaS), Platform as a service (PaaS) and Software as a Service (SaaS), we would like to include an additional suite of services in the IaaS category, given Cloudflare's particular service model.

In the IaaS category, Cloudflare considers Network as a Service (NaaS) to be an important cloud service model. NaaS allows customers to operate their own networks without maintaining their own networking infrastructure. NaaS vendors provide networking functions using software,

[1] For more information on Cloudflare's service see Cloudflare.com's website

essentially allowing companies to set up their own networks entirely without having to own hardware. NaaS can replace virtual private networks (VPNs), multiprotocol label switching (MPLS) connections, or other legacy network configurations, as well as on-premise networking hardware such as firewall appliances and load balancers. A newer model for routing traffic and applying security policies, NaaS has had a major impact on enterprise networking architecture.

Likewise, Secure Access Service Edge (SASE) products and services, which combine network security functions with software-defined networking, are considered an important model within a cloud provider's infrastructure. These services offer customer employees the ability to authenticate and securely connect to internal resources from anywhere, and provide better control over and visibility into the users, and to track data accessing a large network — vital capabilities for modern, globally distributed workforces. Although SASE products include a range of NaaS products, they are considered their own class of services.

Cloudflare strongly feels that businesses and consumers should be able to choose the best cloud services for their needs. That means that they should be empowered to evaluate offerings and should not face artificial barriers to using services from a range of providers. Our network is therefore designed to allow customers to connect their data between people, apps, data, devices, networks, and clouds in a fully interoperable way, providing both security and performance. By its nature, this is a pro-competitive approach and an antithesis to the way the dominant cloud providers (often called hyperscalers) have traditionally run their businesses, which is based on vendor lock-in and uncompetitive bundling practices that make it near impossible to mix and match competitive offerings across the cloud space.

Although our consumers want to construct systems that are made up of their preferred solutions, they are often thwarted in doing this by the business practices of large providers that are able to leverage successful products to expand usage of less developed products. Consumers face operational challenges such as lack of interoperability or cloud ecosystems that intentionally preference particular tools. In addition, economic challenges such as technical barriers or the use of cloud credits can lead them to being locked into their existing providers' ecosystems, with little ability to switch. We believe the analysis around the use of credits in particular, is lacking thus far and needs further regulatory consideration.

III. Cloud marketplaces, combined with committed spend discounts, entrench the market positions of the hyperscalers

As described in both the PDR and associated Appendices U and V, cloud providers offer discounts, which are conditional on customers committing to a certain level of spend. These are often in the form of cloud credits which encourage customers to concentrate their spend with one cloud provider. Certain Committed Spend Discounts (CSD) incentivise customers to buy third party services in hyperscaler marketplaces, increasing their advantages and leveraging their market power against those who choose not to join their marketplaces. They also require

those customers to build on the larger providers' cloud infrastructure services in order to join their marketplaces.[2]

We believe that the CMA has failed to recognise the extent to which the use of CSDs for purchases in the marketplaces distorts related cloud services markets and ultimately results in fewer rivals that can compete profitably against the hyperscalers, the reasons for which we highlight below. We also provide additional evidence of our findings in Appendix A.

Our customers have identified a three step process that hyperscalers use to exert their influence through marketplaces.

a) Hyperscalers require third party vendors to build on their infrastructure in order to sell through their marketplace, restricting their activity with contractual terms

Hyperscalers use their market power to ensure vendors develop their applications and services on the hyperscalers' infrastructure. First, hyperscalers only allow vendors that have built on the hyperscaler's infrastructure into their marketplaces. This strategy directly benefits the hyperscalers. As the use of a third party vendor increases, so does that third party vendor's use of the hyperscalers' infrastructure. A successful third party product will therefore result in significant payments to the hyperscaler for benefiting from the hyperscaler's resources.

The approach also has a secondary advantage for the hyperscalers: it provides a high degree of control over third party vendors. By imposing contractual terms on products marketed within their marketplace, the hyperscalers can exercise control over products and partners that potentially pose competition to other sectors of their business. Consequently, hyperscalers play a pivotal, and distorting, role in shaping the development and functioning of partner products that could rival their own offerings.

In addition, coaxing them to build on the hyperscalers' infrastructure makes third parties technically dependent on these hyperscalers and therefore decreases long-term competition in the cloud market. Partners who might otherwise choose to build alternative networks and infrastructure find themselves at a significant competitive disadvantage compared to companies who build on the clouds and avail themselves of the 'Go-To-Market' benefits provided by the marketplaces. Once companies have made the decision to build on, and become dependent on, the hyperscalers, it will be difficult for them to try to compete against products or services offered by these, both for technical reasons and for fear of retribution. As a result, the market is deprived of potentially superior products and technology, as well as the alternative infrastructure that these companies would otherwise have attempted to create.

[2] See Committed Spend Agreements working paper, page 11
https://assets.publishing.service.gov.uk/media/664f0300f34f9b5a56adccfd/Committed_spend_agreements_working_paper.pdf

b) Hyperscalers encourage customers to make large spending pre-commitments

As identified in the PDR, hyperscalers provide significant “discounts” to customers who make large minimum spending commitments over long term contracts. Spending pre-commitments can run into the billions of dollars and tend to be made on a “use-it-or-lose-it” basis. This means that if customers do not use all of the capacity they have purchased, they lose it at the end of the contract term, without reimbursement. The CMA itself has also found evidence that businesses use certain cloud providers with the sole purpose of meeting their committed spend targets.

c) Hyperscalers extend spending pre-commitments to purchases of partner-products in the marketplace

Hyperscalers justify these large spending amounts by offering the ability to use any unspent amounts as credits for purchases of any product in the marketplace. Businesses agree to these deals because of the perception that they are getting more value for their contracts, even though services sold in the marketplace are often more expensive than they would be if purchased independently.

In practice, this approach gives the hyperscalers significant power to demand that smaller vendors use their infrastructure. Vendors that do not operate on hyperscaler infrastructure, and therefore are not in hyperscaler’ marketplaces, are rendered ineligible to bid for a customer’s business because of the way in which customers budget for services.

Customers with an excess budget at the end of their fiscal year use cloud credits to secure pre-approved budgets for the following year, which forces them to buy only from vendors that are marketplace participants the following year as well. They are in effect using the hyperscaler’s marketplace as a bank, and the loan terms tie them to purchase from the hyperscaler's dependent ecosystem. Indeed, the PDR cites the Jigsaw evidence to identify this approach as one of the main ways that CSDs influences customer behavior, noting in paragraph 7.59(b):

> *There is evidence from across the sample that the existence of behaviour-based discounts influences how companies actually use the services offered by their cloud provider. In particular, some research participants described how their companies use certain cloud services, not because there is a business or an IT need, but for the sole purpose of meeting committed spend targets.*

In considering the effect on competition, the PDR primarily considers the effect of CSDs on other large cloud providers. In practice, however, the ability to use CSDs for products in the marketplace, combined with the way customers use the CSDs, give the hyperscalers tremendous power to demand that a range of products be developed on their infrastructure so that they can be sold in the marketplace. Hyperscalers are using long-term agreements with large pre-spending commitments to reinforce lock-in into their ecosystem, not only for the

customers procuring through the marketplace but also for other service providers looking to sell to those same customers.

Hyperscalers also typically require partners' contracts with their own customers to be executed on the hyperscaler's paper. In addition, when a partner's product is purchased on the hyperscaler's marketplace, the hyperscaler handles the actual payment to the partner. This gives hyperscalers complete insight into third party vendors' commercial arrangements with their own customers, including pricing and payment, positioning them to potentially compete against those third party vendors for the most interesting and valuable deals.

Although marketplaces may provide some efficiencies for businesses and customers, vendor lock-in issues are problematic, particularly for customers that would otherwise use products that are not in the marketplace. Those customers are unable to benefit from other vendors' products and pricing because the unused portions of their credits make competing products in the marketplace essentially free or available at reduced cost. We respectfully submit that, in its provisional findings, the CMA has failed to take into account evidence from vendors other than that of the hyperscalers. This has skewed the data and therefore its perception that rival cloud providers are able to compete profitably. We would therefore urge the CMA to review its provisional decision (see Appendix A for additional evidence).

IV. Software Licensing practices

The CMA's decision to investigate the distortion of competition in the cloud market from software licensing practices also reflects concerns we have heard from our customers. Bundling practices increasingly 'lock in' customers to their current vendors for their additional service needs (which go beyond those they originally signed up for).

Practices of bundling of additional products to their productivity suite, have been prevalent in the markets for video conferencing, gaming, and recruiting, among others. These are not new and have already been raised by and with European regulators.[3] The recent complaint[4] filed by Google with the European Commission relating to Microsoft's Licensing practices further highlights the extent to which Microsoft has locked in its customers pushing them to solely rely on its products and services. We list our specific concerns in relation to software licensing practices in Appendix B.

V. Technical barriers restrict businesses' ability to use services outside a cloud service provider's ecosystem

The CMA has provisionally found that there are Adverse Competitive Effects (AECs) arising from certain features in the cloud services markets in the UK. This is in line with what we have

[3] https://cispe.cloud/executive-summary-of-cispe-complaint-against-microsoft/

[4] https://cloud.google.com/blog/topics/inside-google-cloud/filing-eu-complaint-against-microsoft-licensing

heard from our customers, who face significant technical barriers to multi-cloud and switching, which has led to entrenched market power for hyperscalers. Issues around interoperability and technical features that hinder the ability of customers to switch providers are central in contributing to vendor lock-in. In particular, applications from large cloud providers that require customers to rely on certain identity providers or that limit customers' ability to use their own cryptographic certificates to secure their applications pose problems. The effect of such an approach is that *only* the provider of an application can monitor and audit the application for security risks. Not only does this limit the use of alternate cloud security vendors, it also means that a customer has no choice but to rely on the cloud provider's security to use the business application.

Ensuring interoperability for cloud-based security products is not only important for expanding customer choice, it is critical to helping secure businesses from potential cyberattacks. Businesses often look for diversity in their security vendors to'layer' their cybersecurity in order to reduce the risk of putting all their trust in a single vendor. We elaborate on our specific concerns in Appendix B.

We therefore agree with the CMA's provisional conclusion that technical barriers to interoperability created by hyperscalers disincentivise customers from switching and multi-cloud and that necessary action should be taken to mitigate the negative impacts on competition in the cloud services market.

VII. Conclusion

In respect of cloud services, we look forward to engaging with the CMA on any possible remedies that might mitigate detrimental effects on our customers, ahead of its final decision.

With regard to our concerns outlined above, we would make the following initial recommendations. We have proposed further remedies for consideration in Appendix C:

1. **Technical barriers:** Specifically require cloud providers to make their security features easy to interoperate with other third party providers.
2. **Committed Spend Discounts:** Prohibit practices on marketplaces designed solely to benefit hyperscalers. Marketplaces should include products and services from all third-party providers, and not only those who build on hyperscaler infrastructure. The CMA should also prohibit the use of artificial contractual barriers to allow customers to choose the best fit for their needs, while enjoying interoperability between the tools they purchase..
3. **Software Licensing Practices:** Restrict bundling of security services and ensure any new security products are offered at a fair market price and in a transparent manner, rather than being bundled below cost with existing products in markets where hyperscalers already have a dominant position.

We welcome a further discussion with the CMA about the issues we have identified above.