Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109 USA
415.436.9333
eff.org

Federal Trade Commission **June 21, 2023**
April Tabor, Secretary
600 Pennsylvania Ave NW
Washington DC 20580

Re: FTC-2023-0028, Solicitation for Public Comments on the Business Practices of Cloud Computing Providers - Comments of the Electronic Frontier Foundation

Dear Ms. Tabor, Commissioners and Staff of the FTC,

The Electronic Frontier Foundation commends the FTC for investigating the business practices of cloud computing providers. EFF is a non-profit civil liberties organization with more than 28,000 dues-paying members. EFF has worked for 33 years to ensure that technology supports freedom, justice, and innovation for all people of the world. EFF supports vigorous enforcement of antitrust and consumer protection laws, informed by technical expertise.

Cloud computing is an important, indeed essential, part of doing business today. Most businesses require an internet presence, and to be on the internet at any sort of scale requires cloud computing services. Without these services, the details of building and maintaining internet infrastructure can easily overwhelm the real job that people want to do. Without cloud computing services, small businesses simply cannot compete against large ones. Cloud computing keeps the technical infrastructure of internet presence from being a moat around well-capitalized businesses.

Our comments address two issues that should inform the Commission's inquiry: Amazon's dominant role in an important sector of the cloud computing market, and the importance of interoperability to reduce the costs of switching and combining services.

1. The Market for Cloud Computing Services to Small User-Facing Websites, and Amazon's Dominant Role in That Market

Amazon, the largest cloud computing provider, consistently controls nearly half of overall market share for public infrastructure as a service (IaaS).[1] Yet that number, and the presence of competitors in the broader market for IaaS, does not capture how pervasive Amazon is in the digital lives of most Americans. Its cloud computing division, Amazon Web Services (AWS), provides the infrastructure for over one million clients, acting as a load-bearing wall of the internet. Worldwide, Amazon's share of the IaaS market is 38.9%,

[1] Edward Jones, "Cloud Market Share: A Look at the Cloud Ecosystem in 2023," Kinsta (Dec. 6, 2022), https://kinsta.com/blog/cloud-market-share/.

with Microsoft's Azure a distant second at 21.1%. In 2021, it accounted for $35 billion in revenue for Amazon, with Microsoft's $19 billion a distant second yet again.[2] In the United States, around 41% of the top 100,000 websites use Amazon's services. In the top 10,000 it's almost 53%.[3]

For the average person, that means that interaction with Amazon-supported sites and services is inevitable. Netflix, The Guardian, Twitter, and Nordstrom all pay for Amazon's services. The Mississippi Department of Employment Security moved its data management to Amazon in 2021.[4] While the popular conception of Amazon is of its retail and media storefronts, AWS is its most powerful and pervasive product. In fact, if AWS's contributions to Amazon's revenue are removed, the company is no longer profitable.[5]

In other words, AWS provides the profit that enables Amazon's predatory conduct in retail. And because most people do not know or look into whether the site they're using is an AWS customer, even those looking to "vote with their feet" by not purchasing items on Amazon.com will still contribute to those profits.

In 2019, journalist Kashmir Hill embarked on a project where she stopped use of the services of of five Big Tech companiesfor a week each. For Amazon, her headline speaks volumes: "I Tried to Block Amazon From My Life. It Was Impossible."[6] Hill had a device set up that would block her access to any website with an IP address controlled by Amazon. Over the course of her week without Amazon, Hill had over 23 million IP addresses blocked and even then she discovered it wasn't catching all of them, since many AWS customers route traffic through services like Cloudflare that obscure their IP addresses. Many government agencies use AWS, which once again makes not interacting with the service impossible for most.

Another example highlighted by Hill was that the secure messaging service Signal had to give in to demands from Amazon to stop disguising its traffic, a technique Signal used

[2] "Gartner Says Worldwide IaaS Public Cloud Services Market Grew 41.4% in 2021," Press Release (June 2, 2022), https://www.gartner.com/en/newsroom/press-releases/2022-06-02-gartner-says-worldwide-iaas-public-cloud-services-market-grew-41-percent-in-2021.

[3] "Amazon Usage Statistics," BuiltWith, https://trends.builtwith.com/hosting/Amazon (accessed June 21, 2023).

[4] "Mississippi Department of Employment Security Cuts Infrastructure Costs by 72% on AWS," AWS Case Study (2021), https://aws.amazon.com/solutions/case-studies/mississippi-department-of-employment-security-case-study.

[5] Gennaro Cuofano, "Amazon Revenue Breakdown," FourWeekMBA (June 6, 2023), https://fourweekmba.com/amazon-revenue-breakdown/.

[6] Kashmir Hill, "I Tried to Block Amazon From My Life. It Was Impossible," Gizmodo (Jan. 22, 2019), https://gizmodo.com/i-tried-to-block-amazon-from-my-life-it-was-impossible-1830565336.

to evade shutdowns by repressive governments.[7] Hill was told that Signal had to do what Amazon asked because "there's no good alternative."[8]

In addition to its ubiquity, stories like Hill's illustrate Amazon's market power and its inherent dangers of censorship and uniformity. AWS has terms of service that allow it to make potentially anticompetitive demands of its customers, including rules surrounding what kind of content it will and will not host.[9] Amazon's rules give the company significant discretion—which it used against Signal.

This centralization of power over the content of the world's most-viewed websites has the danger of homogenizing the web. Those are the sites most likely to show up at the top of a search. If, hypothetically, Amazon decided to crack down on hosting sites with information on abortion—as some U.S. state governments want it to do—then people looking for legal content on that topic might be hard pressed to find it. Most will get whatever content Amazon has determined is low risk.

Amazon's market position also puts less popular websites at risk of censorship. While The Guardian may challenge Amazon's policies and decisions on content, many others will not feel comfortable doing so. Amazon's dominance creates a single point of failure for the rights of millions. In addition to data about the actual customer, Amazon has access to the information of a customer's users, so long as the customer has agreed.[10] If law enforcement or any other government actor requests information from Amazon, they could sweep up all sorts of things that they should not have access to.

AWS's particular dominance in services to websites gives Amazon a dangerous amount of power over how most people experience the internet and what they see and say on it. Content moderation at the infrastructure level carries heightened risks to human rights: overblocking of non-objectionable content, a lack of meaningful notice and appeal process, capture by repressive governments and private interests bent on censorship, and the widely recognized challenges of performing content moderation on a global scale.[11] Because cloud computing services are increasingly essential to internet commerce, a dynamic and fair cloud computing market must be accessible to all, regardless of the popularity of a customer or their message.

[7] Rhett Jones, "Amazon Bends the Knee to Autocrats, Threatens to Cut Off Signal for Using Anti-Censorship Technique," Gizmodo (May 1, 2018), https://gizmodo.com/amazon-bends-the-knee-to-autocrats-threatens-to-cut-of-1825697153.

[8] Hill, *supra* note 6.

[9] "AWS Acceptable Use Policy," Amazon, https://aws.amazon.com/aup/ (updated July 1, 2021).

[10] "Data Privacy FAQ," Amazon, https://aws.amazon.com/compliance/data-privacy-faq/.

[11] "Protect the Stack," https://protectthestack.org/.

If we are to avoid censorship at the infrastructure level, competition and customer choice in cloud computing services is essential. That's why Amazon's market share among top websites, and the actual or latent editorial power it possesses over those websites, should be a factor in any analysis of Amazon's market power in IaaS.

2. Commission Policy Should Make it Easier For Customers to Switch Cloud Services Providers And Combine Services From Multiple Providers.

Businesses of all sizes face high barriers to moving between different cloud services providers or using services from different providers. High switching costs and barriers to combining services from different providers are common across the major providers.

Some of the biggest barriers to easy switching come from the know-how required to switch and the cost of administering disparate systems. The user interfaces, administration tools, and configuration processes of cloud services providers vary greatly. Although a choice of approaches is generally good for customers, running websites and services on third-party infrastructure involves building institutional knowledge that is not easily transferable to a different provider. This makes switching providers prohibitively expensive for many businesses. Switching requires learning how to configure and maintain systems running in a new infrastructure. And moreover, transitioning a functioning business means learning a new system, learning the technology for transferring data and software to the new system, all while continuing to operate an existing system.

Cloud services providers may also charge high fees to export data. The Commission should pay close attention to whether these fees reasonably reflect the costs involved.

For a business customer, using services from different providers involves overcoming many of the same barriers. This may be done for redundancy in the case of outages, or simply to use the best tool for a given task.

The largest cloud services providers offer many services and sub-services outside of their basic service set. AWS, for example, has 240 different options.[12] While convenient, these broad menus of services offer opportunities for product tying and predatory pricing.

The Commission should pursue policies that promote interoperability between the offerings of the various cloud services providers. Interoperability reduces switching costs, which increases the market incentives of each provider to compete on the quality and price of their offerings, including offering better privacy, security, and reliability. Pro-interoperability policies can and should include a mix of approaches: encouraging the use of open standards and protocols for communication between services, creating incentives for providers to offer robust, consistent, and well-documented technical interfaces to their

[12] "AWS Cloud Products," https://aws.amazon.com/products/ (accessed June 21, 2023).

services, ensuring that competing providers can use those interfaces on equal terms.[13] Another is securing commitments to refrain from asserting claims under laws like the Computer Fraud and Abuse Act and the Digital Millennium Copyright Act against legitimate competing providers that arise from interoperating with the incumbent provider.[14]

The Commission can use a variety of tools to pursue these policies. One option is requiring providers with some measure of market power to interoperate effectively with the offerings of competing providers. But interoperability policies can also form part of the remedies sought in court actions under the FTC Act or in negotiated settlements.

EFF thanks the Commission for its attention to these issues.

Respectfully submitted,

Mitchell L. Stoltz
Competition Director
Katharine Trendacosta
Associate Director of Policy and Activism
Electronic Frontier Foundation

[13] Bennett Cyphers and Cory Doctorow, "Privacy Without Monopoly: Data Protection and Interoperability," Part 3 (Feb. 12, 2021), https://www.eff.org/wp/interoperability-and-privacy.

[14] Cyphers and Doctorow, *supra* note 13, part 3.1.