

Solicitation for Public Comments on the Business Practices of Cloud Computing Providers

The staff of the Federal Trade Commission is inviting public comments about the practices of Cloud Computing Providers and their impact on end users, customers, companies, and other businesses across the economy. FTC staff is studying a wide array of issues related to market power, business practices affecting competition, and potential security risks. Staff is also interested in cloud computing with respect to specific industries, including but not limited to healthcare, finance, transportation, eCommerce, and defense. For these specific sectors or more broadly, are there particular market dynamics shaping business practices that affect competition and consumer protection in cloud computing services? If so, what influences are shaping these market dynamics?

Guidance for submitting comments:

- Staff encourages members of the public to comment on any issues or concerns they believe are relevant or appropriate for our consideration and to submit written data, views, facts, and opinions addressing this subject, including but not limited to the issues posed above. You do not need to answer all questions listed – only the question(s) that you are interested in.
- Do NOT submit sensitive or confidential information. Comments, including anonymous comments, are published on the regulations.gov website and made available to the public.
- If you submit information for the public record as an “anonymous” entity through regulations.gov, please be aware your submission may be published on regulations.gov.
 - (1) Do not provide your email address in the regulations.gov form submission.
 - (2) Do not provide any personally identifying information in your comment or any attached material.
 - (3) Everything you submit can be made public, and you may be held liable or accountable for anything you share.

Questions

Market Power and Business Practices Affecting Competition

1. What are the different layers of cloud computing (e.g., infrastructure, platform, software)? To what extent do cloud providers specialize within a layer or operate at multiple layers?
2. Do cloud providers continue to invest sufficient resources in research and development? In which areas are cloud providers investing in most heavily, and why? Are there areas in which cloud providers have not invested sufficient resources, and if so, why?
3. What are the competitive dynamics within and across the different layers of cloud computing? How does service quality vary between providers operating at one layer vs. providers operating at multiple layers?
4. What practices do cloud providers use to enhance or secure their position in any layer of cloud computing? What practices are used by cloud providers that operate at multiple layers to entrench or enhance their position? What are the effects of those practices on competition, including on cloud providers who do not operate at multiple layers?
5. To what extent are cloud customers able to negotiate their contracts with cloud providers? To what extent are customers experiencing take-it-or-leave-it standard contracts? How does the ability to negotiate depend on the size of the customer, the sensitivity of the data, the purpose for which the data will be used, or other factors?

6. What incentives are cloud providers offering to customers to obtain more of the cloud services they need from a single provider? Are cloud providers linking, tying, or bundling their cloud services with other services?
7. What are the trends in pricing practices used by cloud providers? How have pricing practices made it easier or more difficult for customers of cloud services to understand and control the amount of money they spend on cloud services?
8. To what extent do cloud providers offer products based on open-source software?
 - a) What is the impact of such offerings on competition?
 - b) How have recent changes to the terms of open-source licenses affected cloud providers' ability to offer products based on open-source software?
9. What types of products or services do cloud providers offer based on, dependent on, or related to artificial intelligence (AI)? To what extent are AI products or services dependent on the cloud provider they are built on, or are they cloud-agnostic? How does the use of AI affect competition among cloud providers today and into the future?
10. What barriers (e.g., contractual, technological, or other), if any, exist to offering services that compete with individual services offered by cloud infrastructure providers (e.g., hosted databases, Content Delivery Networks, etc.)? What costs do cloud customers face in:
 - a) switching software services?
 - b) using multiple cloud providers?
 - c) porting their data from one cloud provider to another? How important is data portability to competition and to entry?

Security Risks

11. To what extent are particular segments of the economy reliant on a small handful of cloud service providers and what are the data security impacts of this reliance?
12. Do cloud providers compete on their ability to provide secure storage for customer data? Do cloud providers compete on the understandability of the user interface or APIs used to configure security and access features to avoid inadvertent exposure of customer data?
13. What diligence regarding data security do potential customers conduct when selecting a cloud provider?
14. What representations do cloud providers make to their customers about data security or interoperability? What information do cloud providers provide to potential customers such that potential customers can evaluate the providers' security measures and interoperability capabilities?
15. Do cloud vendors provide types of customers with different information during diligence than they provide to other types of customers? If so, does this vary by contracts or contractual provisions, or by their ability to monitor their performance and security?
16. Under what circumstances do cloud vendors identify security risks related to their customers' security design or implementation/configuration (e.g., a publicly accessible data store containing personal information) and notify customers of that risk?
 - a) How frequently does this occur?
 - b) In this scenario, when and how does the vendor notify the customer?
17. What effect does security-related regulation (e.g., GLBA Safeguards Rule, HIPAA Security Rule, etc.) have on market dynamics?
18. Can companies comply with contractual obligations to do due diligence on the security of third party cloud providers to whom they entrust information to ensure that those third party cloud

providers implement appropriate security measures, and to monitor third party cloud providers' security on an ongoing basis? If so, how do companies do this due diligence?

19. How is responsibility for the security of consumers' personal information allocated between cloud vendors and cloud customers (e.g., allocated by standardized vendor-provided contract or by custom contract)?
 - a) How is this allocation conveyed in specific contractual provisions?
 - b) Is this allocation of responsibility clear? If not, why?
 - c) Is this allocation of responsibility effective at protecting the information? Why?
20. How is responsibility for responding to a breach of data stored in the cloud or other security incident allocated between cloud vendors and customers (e.g., allocated by standardized vendor-provided contract or by custom contract)?
 - a) How is this allocation conveyed in specific contractual provisions?
 - b) Is this allocation of responsibility clear? If not, why?
 - c) Is this allocation of responsibility effective at facilitating prompt and legally-compliant data breach response? Why?