

[Blogs](#)

March 29, 2023

FTC Requests Comments on Cloud Computing Business Practices With Potential Data Security Impacts



The Federal Trade Commission (FTC) issued a [press release](#) and a [request for information](#) on March 22, 2023, soliciting comments from the public on cloud computing business practices, including issues related to market power, competition, and potential data security risks.

Regarding data security, the request for information seeks to gain insight on cloud computing against the backdrop of [FTC guidance to businesses](#) on steps to secure and protect data stored in the cloud. This request comes amid recent FTC enforcement matters (such as against education technology provider [Chegg](#)) alleging failure to adequately secure data stored on third-party cloud computing services.

Specifically, the FTC seeks comments on topics including the following:

- The extent to which segments of the economy are reliant on a small number of cloud providers, and if so, whether this affects data security.
- Whether cloud providers compete on their ability to provide secure storage for customer data and the understandability of their products' user interfaces for securing data.
- What diligence potential customers conduct regarding data security when choosing a cloud provider.
- What representations cloud providers make about data security to customers, and what information they provide to potential customers to enable them to evaluate data security and interoperability.
- Whether cloud providers share different information about data security with different types of potential customers, and if so, on what basis is the different information provided.
- The circumstances under which cloud providers identify risks related to customers' implementation or configuration of their cloud services and notify such customers.
- The effect of security-related regulations such as the GLBA Safeguards Rule and the HIPAA Security Rule on "market dynamics."
- Whether customers can comply with their own contractual obligations to conduct due diligence, and if so, how they conduct such diligence, on the security practices of cloud providers.

- Whether customers can monitor security practices on an ongoing basis.
- The contractual allocation between cloud providers and their customers for securing personal information, and the clarity and effectiveness of securing said information.
- The contractual allocation between cloud providers and their customers for responding to a breach, and the clarity and effectiveness of the allocation in securing personal information.

The FTC's requests for information on other aspects of cloud computing practices include topics such as whether cloud customers can negotiate their contracts with cloud providers or whether said providers are accepting take-it-or-leave-it standard contracts; incentives providers offer customers to obtain more of their cloud services from a single provider; and the types of products or services cloud providers offer based on, dependent on, or related to artificial intelligence (AI) and the extent to which those products or services are proprietary or provider-agnostic.

Companies who provide or use cloud computing services may want to comment to the FTC about these practices to help the FTC gain accurate insights. Comments may be submitted until May 22, 2023. Submitted comments will be public and will be posted on *Regulations.gov*, but comments can be submitted anonymously.

Update: The FTC extended the comment period on the Request for Information by 30 days and is now accepting comments until June 21.

Explore more in

[Privacy & Security](#)