Before the
FEDERAL TRADE COMMISSION
Washington, D.C. 20580

COMMENTS

of

PRIVACY FOR AMERICA

on the

Solicitation for Public Comments
on the Business Practices of Cloud Computing Providers, FTC-2023-0028-0001

Counsel:
Stuart P. Ingis
Tara Sugiyama Potashnik
Rob Hartwell
Allie Monticollo
Venable LLP

600 Massachusetts Ave., NW
Washington, DC 20001
202.344.4613

June 21, 2023

I. Introduction

Privacy for America is a coalition of top trade organizations and companies representing a broad cross-section of the American economy. Our membership includes companies and trade associations in the advertising, travel, hospitality, media, financial services, data services, and market research industries, as well as many others. We appreciate the opportunity to provide comments on the Federal Trade Commission's ("FTC" or "Commission") Solicitation for Public Comments on the Business Practices of Cloud Computing Providers ("Solicitation").[1]

Privacy for America supports the congressional creation of a national, preemptive, and comprehensive standard for consumer privacy and data security, as demonstrated in our *Principles for Privacy Legislation* ("Framework").[2] Relevant to the Commission's Solicitation, Privacy for America's Framework calls for flexible data security standards that are tailored to the nature and scope of the covered entity as well as the sensitivity and potential risks of harm to the consumer of the personal information processed by the covered entity.[3] The comments below explain why this flexible, risk-based approach works well in the cloud computing industry by encouraging competition and allowing entities of all sizes to access data security infrastructure that fits their own needs in addition to their customers' needs. We also explain that a one-size-fits-all approach to cloud security standards would be counterproductive to bolstering data protection, because it would diminish access to effective data security for the business community and result in disadvantageous economic and competitive results.

We first provide examples of the varied types of companies that leverage cloud services providers' offerings. We next discuss why the flexible and risk-based approach that cloud services providers ("Providers") take to security improves both competition and the overall level of data security in the marketplace. We conclude by describing how the Framework and the Commission's existing experience can be used as tools to help Congress create a national legislative data security standard to preserve the benefits of cloud computing that we highlight throughout these comments.

I. Cloud services providers offer a range of security features to meet the various needs of their customers.

Providers offer their services to a wide range of clients, from small and start-up companies looking to break into the marketplace to the largest enterprises in the United States. Because some Providers can build their services on common infrastructure and make it available to all their clients, those Providers can offer companies of all sizes off-the-shelf tools to address data security.[4]

---

[1] Solicitation for Public Comments on the Business Practices of Cloud Computing Providers, FTC-2023-0028-0001 (Mar. 22, 2023) (hereinafter, "*RFI*").
[2] Privacy for America, *Principles For Privacy Legislation*, https://www.privacyforamerica.com/overview/principles-for-privacy-legislation/ (last visited Jun. 21, 2023) (hereinafter, "*Privacy For America*").
[3] *Privacy For America* at 28-29.
[4] *RFI*, question 17, 19.

For example, a start-up company may not have the resources to create secure "on-premises" data servers and networks to store the data they hold. That same start-up can access a Provider's effective tools and transfer that infrastructure security responsibility to the Provider, thereby freeing up resources for the start-up and raising the overall level of security in the marketplace. In the same instance, Providers can offer entities in certain highly regulated markets, such as the health care and financial services industries,[5] tools and services to meet the demands that the types of data that they process require in a cost-effective, up to date, and resilient manner. This approach helps provide dependable access to data in a way that increases security in these critical sectors to help protect consumers.

Because Providers can vary the types of security services offered to their clients, as opposed to being required to meet the same mandate for all clients they serve, Providers help companies across the economy access the 21st century's data-driven marketplace in a sensible and risk-based manner. Every company is, at some level, a data-driven company, and Providers offer access to a broad array of expertise, technology, and infrastructure to allow even a sole-proprietor access to the advantages that data can offer.

II. The flexible nature of U.S. data security requirements, along with the range of security features offered by cloud services providers, foster competition and innovation by allowing entities of all sizes to compete.

The ability of Providers to offer flexible security solutions to their clients is grounded in the concept of "shared responsibility."[6] By taking responsibility for the security of the underlaying infrastructure of the cloud, and helping their clients implement appropriate security measures for the data they process in a Provider's cloud, Providers and their clients are able to determine what level and types of security tools should apply to the volume of data, type of data, and use cases the data processing will encompass to help address reasonable threats to security.

An example of how this shared responsibility model works in practice is the split between the physical security of cloud hardware and the provision of user access to the data a Provider's client stores in the cloud. When a new apparel company wants to create a database to store customer names, email addresses, shipping addresses, and other information, it can do so on a server in its own warehouse, or it can leverage a Provider to store and process that data. The benefits of the cloud security model allow that new company to access hardware, software, and other information technology resources that would otherwise be cost prohibitive.[7] At the same time, the Provider can work with its client to implement the right security tools for the client's needs, with the client selecting the appropriate level of user access and encryption based on its own assessment of its data assets, how it needs to process that data, and which employees should be able to access that data. Thanks to the flexible approach of cloud security, a new competitor is able to be in the marketplace with market-standard security for data about its customers that a company of that size would be unable to achieve without the services offered by Providers.

---

[5] 15 C.F.R. §§ 314.1 *et seq*.; 45 C.F.R. §§ 164.302 *et seq*.
[6] Amazon, *Shared Responsibility Model* (2023), https://aws.amazon.com/compliance/shared-responsibility-model/.
[7] Microsoft, *Shared Responsibility for Cloud Computing* (2019), Shared Responsibility for Cloud Computing-2019-10-25.pdf (microsoft.com).

Consumers can shop with more trust and confidence and reap the benefits of competition such as lower prices and greater choice.

Additionally, large enterprises that process much more data than an apparel start-up can use a Provider's services to help lower their information technology budgets without sacrificing security for the data they hold about consumers, thanks to the ability of Providers to customize solutions. A financial institution, for example, can work with a Provider to use both in-house and cloud infrastructure to create efficient data flows to improve the financial institution's offerings to consumers, while using the most efficient data security services to protect the data it maintains to operate the various aspects of its company. This mix of services offered by Providers, and the ability of Providers to work with their clients to assess the risk profile of the data that will be stored with the Provider, aids all involved parties and empowers them to address those risks together.

The overall level of security in the marketplace is increased due to flexible, risk-based security practices for Providers. Because Providers are responsible for the security of the cloud itself, and because they are not required to apply the same data security tools, procedures, and requirements to all customers, any company using a Provider's services is able to receive an appropriate level of protection for that aspect of the business. Additionally, given the variety of expertise and tools offered to a Provider's clients, each company is able to customize their suite of security protections to the industry and consumer expectations relevant to their business.

III. The history of flexible data security standards in the United States has bolstered the economy, and any new requirements that may apply to cloud services providers should build on that example through national, preemptive privacy and data security legislation passed by Congress.

The Privacy for America Framework, as well as the Commission's prior experience in data security rulemaking, make clear why any attempt to address data security for Providers should create a structure that rewards good-faith compliance with risk-based security standards.[8] Restrictive, one-size-fits all mandates will both fail to provide needed flexibility to incentivize companies to leverage the tools offered by Providers and harm the overall level of security in the marketplace. Congress should create a flexible and risk-based approach to help ensure companies of all sizes have access to robust data security services at a price point that is possible for them.

A principles-based approach would allow companies to prioritize security in ways that make sense given the nature of the data they handle, their size and capabilities, and the risk of harm to consumers based on the data that will be processed by the entity. The Commission should take note that flexible standards for the various ways that companies create data security programs allow them to optimize and tailor the form and function of their data security programs to the risks they face, as well as new developments in the marketplace and new technologies. For example, the Commission has experience creating such a principles-based approach in the Gramm-Leach Bliley Act Safeguards Rule, which it was directed to create by an act of

[8] *Privacy for America*, 28-29.

Congress.[9] In the cloud security context, such an approach—with legislation enacted by Congress setting a clear intent for flexible data security standards—would allow both large and small businesses to secure information in an appropriate manner and weigh Providers' security tools against the risk of potential harm to individuals. This type of risk-based framework is especially important given the potential scope of the types of customers that may leverage a Provider's services. Applying the same one-size-fits-all security requirements to mom-and-pop corner stores and Fortune 50 companies would not be appropriate, reasonable, or responsible. The Commission should focus its efforts on helping Congress set forth a risk-based framework to evaluate reasonable security procedures that are tailored to the nature of the security risk presented by a particular context and business model.

The results of this request for information should help inform the Commission in its potential work with Congress on the creation of national data privacy and security legislation. The Commission should support the creation of a national data security standard through legislation that works across all actors in the marketplace, a result that can be best achieved through the legislative process. Consumers should have the opportunity to benefit from secure data from a wide range of companies across all sectors of the economy, and such companies will likely depend on a Provider for one or more parts of its functionality. A flexible, principles-based, and risk-based approach would not only allow this collaboration to occur now, but it would also help create requirements that would be responsive to changes in market standards, practices, technologies, and other unforeseen realities that may emerge in the future.

* * *

Thank you for the opportunity to provide comments on this request for information. Please contact us with questions regarding this submission.

Sincerely,
Privacy for America

[9] 16 C.F.R. § 314.1 *et seq*.