epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

☎ +1 202 483 1140
📠 +1 202 483 1248
🐦 @EPICPrivacy
🌐 https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

Federal Trade Commission

on

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

Docket ID FTC-2023-0028230407-0093

June 21, 2023

The Electronic Privacy Information Center (EPIC) submits these comments in response to the Federal Trade Commission (FTC)'s recent request for information regarding the business practices of cloud computing providers.[1]

EPIC is a public interest research center in Washington, D.C., established in 1994 to focus on public attention on emerging civil liberties issues and to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation.[2] EPIC has a long history of promoting transparency and accountability for information technology.[3]

EPIC commends the FTC for its interest in the topic of cloud computing. In this comment, EPIC (1) calls attention the growing concentration of the cloud computing market, which is driven in part by the rapid spread of generative AI, and (2) illustrates the urgency of data security concerns in the current cloud computing ecosystem.

In general, EPIC recommends the FTC consult the following resources:

- EPIC, *Generating Harms: Generative AI's Impact & Paths Forward* 57-60 (May 2023), https://epic.org/gai.

[1] Federal Trade Commission, *An Inquiry into Cloud Computing Business Practices* (Mar. 15, 2023), https://www.regulations.gov/docket/FTC-2023-0028

[2] EPIC, *About Us* (2023), https://epic.org/about/.

[3] *See, e.g.*, EPIC, *AI & Human Rights* (2023), https://epic.org/issues/ai/; EPIC, *AI in the Criminal Justice System* (2023), https://epic.org/issues/ai/ai-in-the-criminal-justice-system/; EPIC, *Generating Harms: Generative AI's Impact & Paths Forward* (2023), https://epic.org/wp-content/uploads/2023/05/EPIC-Generative-AI-White-Paper-May2023.pdf; EPIC, *Screen & Scored in the District of Columbia* (2022), https://epic.org/wp-content/uploads/2022/11/EPIC-Screened-in-DC-Report.pdf; Comments of EPIC, *In re Privacy, Equity, and Civil Rights Request for Comment* (Mar. 6, 2023), https://epic.org/wp-content/uploads/2023/03/EPIC-comments-NTIA-DiversityEquityCivilRights-RFC.pdf.

- Amba Kak and Sarah Myers West, *AI Now 2023 Landscape: Confronting Tech Power*, AI Now Institute 15-33 (Apr. 11, 2023), http://ainowinstitute.org/2023-landscape.
- Staff of Subcomm. on Antitrust, Com., & Admin. L. of the H. Comm. on the Judiciary, *Investigation of Competition in Digital Markets: Majority Staff Rep. and Recommendations,* 117th Cong. 95 (July 2022), https://www.govinfo.gov/content/pkg/CPRT-117HPRT47832/pdf/CPRT-117HPRT47832.pdf.
- Sarah Myers West, 'Competition Authorities Need to Move Fast and Break up AI', Financial Times (Apr. 17, 2023), https://www.ft.com/content/638b5be7-fab7-4fe6-a0cf-7dabefcdd722.
- Lina M. Khan, *Amazon's Antitrust Paradox*, 126 Yale L. J. 710 (2017), https://www.yalelawjournal.org/pdf/e.710.Khan.805_zuvfyyeh.pdf.

I. The Cloud Computing for AI Market Is Highly Concentrated in a Small Number of Major Providers

In view of the rapid spread and increased funding of generative AI, EPIC urges the FTC to focus especially on the business practices of dominant cloud computing providers like Microsoft, Facebook, and Alphabet that are profiting and stand to further profit from increased AI deployment.

Developing, training, using, and maintaining generative AI tools is a resource-intensive endeavor. In addition to the environmental costs, administering generative AI is incredibly expensive and demands vast computing resources. Experts have estimated that the costs of operating ChatGPT, including the underlying computing power, run to $700,000 a day[4]—a figure that contributed to an estimated $540 million loss for Open AI[5], creator of ChatGPT, in 2022. Open AI has received investment from Microsoft to the tune of more than $10 billion dollars, including hosting with Microsoft Azure,[6] one of a few major providers of cloud computing resources.[7] OpenAI will reportedly be seeking additional investment of $100 billion dollars.[8]

These astronomical costs mean that large-scale AI models are frequently developed and operated by the few Big Tech firms with the resources to handle them—as well as the public relations and lobbying power to effectively promote those same models. Amazon Web Services,

[4] *See, e.g.*, Hasan Chowdhury, *ChatGPT costs a fortune to make with OpenAI's losses growing to $540 million last year, report says*, Business Insider (May 5, 2023), https://www.businessinsider.com/openai-2022-losses-hit-540-million-as-chatgpt-costs-soared-2023-5#:~:text=Last%20month%2C%20Dylan%20Patel%2C%20chief,costs%20involved%20with%20computing%20power.

[5] *See id*.

[6] *See* Rahul Kumar, *Cloud Market Share 2023: An Overview of Growing Ecosphere*, WPOven (Sept. 19, 2022), https://www.wpoven.com/blog/cloud-market-share/.

[7] *See id*.

[8] *See id.*

Microsoft Azure, Google Cloud, and Oracle Cloud hold most of the cloud computing resources and enjoy a consolidated market.[9]

In addition to their resource-intensive development of Generative AI models, these same large firms are some of the primary providers of off-the-shelf AI models and related cloud computing services. Although these companies often profit off narratives touting the "open source" nature of generative AI, the markets they dominate are in fact top-heavy and opaque.

As President Biden explained when announcing the Executive Order on Competition, the "American information technology sector has long been an engine of innovation and growth, but today a small number of dominant Internet platforms use their power to exclude market entrants, to extract monopoly profits, and to gather intimate personal information that they can exploit for their own advantage."[10] EPIC urges the administration to investigate anticompetitive behavior in the cloud computing for AI industry and to avoid unintentionally increasing the market share of dominant providers through government policies and acquisitions.

II. There is Broad Agreement on Data Security Best Practices for Cloud Services, But Implementation Responsibility is Ambiguous

EPIC commends the Commission for its attention to data security in this RFI. Proliferation of cloud services was recently reported to be among the top deterrents preventing improvements to data breach response efforts by 58% of IT security, privacy, and compliance professionals;[11] this was a greater percentage than proliferation of mobile devices or even the lack of security processes for third parties with access to data.[12] Last year, it was estimated that 60% of enterprise data would be stored in the cloud in 2022.[13] The Commission's emphasis on this issue is timely.

Indeed, the White House recently called for a rebalancing of the responsibility to defend cyberspace in its National Cybersecurity Strategy, "shifting the burden for cybersecurity . . . onto the organizations that are most capable and best-positioned to reduce risks for all of us."[14] The strategy

[9] *See* Staff of Subcomm. on Antitrust, Com., & Admin. L. of the H. Comm. on the Judiciary, *Investigation of Competition in Digital Markets: Majority Staff Rep. and Recommendations,* 117th Cong. 95 (July 2022), https://www.govinfo.gov/content/pkg/CPRT-117HPRT47832/pdf/CPRT-117HPRT47832.pdf.

[10] Executive Order on Promoting Competition in the American Economy (July 09, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/07/09/executive-order-on-promoting-competition-in-the-american-economy/

[11] *See* Ponemon Institute, Ninth Annual Study: Is Your Company Ready for a Big Data Breach?, sponsored by Experian Data Breach Resolution 32 (Feb. 2022), https://www.experian.com/content/dam/marketing/na/data-breach/reports/9th-Annual-Data-Breach-Preparedness-Study-Ponemon.pdf ("A sampling frame of 15,251 US and 12,880 EMEA IT and IT security, compliance and privacy professionals, who are involved in data breach response plans in their organizations were selected as participants to this survey.").

[12] *See id*. at 9.

[13] *See, e.g.*, Simon Jelley, Data Management in a Multi-Cloud World, Forbes (June 7, 2022), https://www.forbes.com/sites/forbesbusinesscouncil/2022/06/07/data-management-in-a-multi-cloud-world/?sh=5c2d69c41777 (citing to Statista, Share of corporate data stored in the cloud in organizations worldwide from 2015 to 2022, https://www.statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data/).

[14] Fact Sheet: Biden-Harris Administration Announces National Cybersecurity Strategy (Mar. 2, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/.

also explicitly called for "expanding the use of minimum cybersecurity requirements in critical sectors,"[15] "promoting privacy and the security of personal data,"[16] and "shifting liability for software products and services to promote secure development practices."[17] This suggests that responsibility should not rest with consumers so much as with cloud-based service providers and their enterprise customers for improving the security of consumer data.

EPIC urges the Commission to consider how it might adequately incentivize service providers and their customers to advance these priorities, especially in light of the wide adoption of enterprise-level cloud computing and the complications it can introduce to breach response efforts.

Responsive to Questions 14 and 19

Companies in the cloud-based services marketplace openly discuss the variety and ambiguity of allocation of responsibility for data security in cloud services.[18] Unless each party is clear on what its responsibilities are to protect consumer data, it is possible that neither party will implement the

[15] *Id*. pillar one: "Defend Critical Infrastructure."

[16] *Id*. pillar three: "Shape Market Forces to Drive Security and Resilience."

[17] *Id*.

[18] *See, e.g.*, Shared Responsibility for Cloud Security: What You Need to Know, Center of Internet Security, https://www.cisecurity.org/insights/blog/shared-responsibility-cloud-security-what-you-need-to-know (last visited June 21, 2023) ("In the public cloud, there's a shared responsibility between the Cloud Service Provider (CSP) and the user (you). Security for things like data classification, network controls, and physical security need clear owners. The division of these responsibilities is known as the shared responsibility model for cloud security."); Kaspersky, What is Cloud Security?, https://usa.kaspersky.com/resource-center/definitions/what-is-cloud-security (last visited June 21, 2023) ("With cloud computing, ownership over these components can vary widely. This can make the scope of client security responsibilities unclear."); Sharon Farber, Cloud Data Security & Protection: Everything You Need to Know, Dig Blog (Dec. 7, 2022), https://www.dig.security/post/cloud-data-security-everything- you-need-to-know ("At a high level, the cloud provider is responsible for the security *of* the cloud while their customer remains responsible for the security of applications and data *in* the cloud."; "Each service provider and "as-a-Service" model defines the Shared Responsibility differently."); Google Cloud, What is cloud data security? Benefits and solutions, https://cloud.google.com/learn/what-is-cloud-data-security (last visited June 21, 2023) ("Cloud providers and customers share responsibility for cloud security. The exact breakdown of responsibilities will depend on your deployment and whether you choose IaaS, PaaS, or SaaS as your cloud computing service model."; "In general, a cloud provider takes responsibility for the security of the cloud itself, and you are responsible for securing anything *inside* of the cloud, such as data, user identities, and their access privileges (identity and access management)."); SailPoint, Data security in cloud computing (Mar. 20, 2023), https://www.sailpoint.com/identity-library/data-security-in-cloud-computing/ ("One data security area that organizations struggle with in cloud computing is who bears the responsibility for security. With on-premises data centers and infrastructure, the responsibility falls to the organization. But in the cloud, they're using vendor's services, and the lines of responsibilities may feel blurry."); Amazon Web Services (AWS), Introduction to AWS Security (Nov. 11, 2021), https://docs.aws.amazon.com/whitepapers/latest/introduction-aws-security/security-of-the-aws-infrastructure.html (outlining via table the responsibilities of customer vs. service provider); Microsoft, Introduction to Azure security (Nov. 15, 2022), https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility (outlining via table responsibilities of customer vs. service provider, which vary based on deployment type); Oracle Cloud Infrastructure (OCI), What is Cloud Security?, https://www.oracle.com/security/cloud-security/what-is-cloud-security/#shared-security-responsibility (last visited June 21, 2023) ("A clear understanding of the shared security responsibility model for all types of cloud services is critical for cloud security programs. Unfortunately, it can also be said that the shared security responsibility model is one of the least understood security concepts in the cloud.").

necessary safeguards, each expecting the other to be responsible. In the end, consumers will be the ones who suffer when their data is breached as a result of these safeguards never being properly implemented. In 2021, nearly one third of 2,800 security professionals and executive leaders surveyed experienced a cloud-based data breach they were legally obligated to report.[19] In the same year, 45% experienced a cloud-based breach or failed audit (regardless of reportable status), up 5% from 2020.[20]

There is general agreement about the safeguards likely to be effective (and therefore those which should be implemented). Commonly recommended data security practices include access controls,[21] encryption,[22] and continuous monitoring.[23] More detailed guidance articulates a total of 18 controls, including training and penetration testing.[24] Any one of these controls may require an explicit allocation of responsibilities.[25] We note that there is significant overlap between what the industry has articulated as best practice here and the issues identified by the Commission through its

[19] *See* Thales News Release, Cloud Data Breaches and Cloud Complexity on the Rise, Reveals Thales (June 7, 2022), https://cpl.thalesgroup.com/about-us/newsroom/thales-cloud-data-breaches-2022-trends-challenges.

[20] *See id*.

[21] *See, e.g.*, AWS (describing offering that can provide "security-specific tools and features across network security, configuration management, access control and data security"); Farber ("You should limit access as precisely as possible, granting each user the least amount of access necessary to complete their job function."); Kaspersky ("*Access controls* are pivotal to restrict users — both legitimate and malicious — from entering and compromising sensitive data and systems. Password management, multi-factor authentication, and other methods fall in the scope of IAM."); Microsoft ("Securing systems, applications, and data begins with identity-based access controls."); OCI ("Proactively protect data with access controls…").

[22] *See, e.g.*, AWS (describing offering that can "add a layer of security to your data at rest in the cloud, providing scalable and efficient encryption features"); Farber ("Nearly every compliance mandate requires organizations to encrypt data-at-rest and in-transit. Encryption makes data unusable unless the recipient has the decryption key."); Kaspersky ("Tools and technologies allow providers and clients to insert barriers between the access and visibility of sensitive data. Among these, *encryption* is one of the most powerful tools available."); Microsoft (describing offering that can "keep your data encrypted at all times"); OCI ("Reduce the risk of a data breach and accelerate compliance in the cloud. Adopt database security solutions that include encryption…");

[23] *See, e.g.*, AWS (describing offering that provides "the visibility you need to spot issues before they impact the business and allow you to improve security posture, and reduce the risk profile, of your environment"); Farber ("Additionally, you need to use threat modeling and threat intelligence for real-time risk detection"); Kaspersky ("Hackers can gain easy access to an entire cloud network via old, dormant accounts through unpatched vulnerabilities."); Microsoft (describing offering that can "monitor your live web applications and automatically detect performance anomalies"); OCI ("Fine-grained access controls, visibility, and monitoring are critical components of today's layered defenses.").

[24] *See* CIS Controls v8 Cloud Companion Guide, Center for Internet Security, available at https://www.cisecurity.org/insights/white-papers/cis-controls-v8-cloud-companion-guide (last visited June 21, 2023) (listing 18 controls, including access controls, continuous vulnerability management, malware defenses, training, and penetration testing). See also, CIS Controls Cloud Companion Guide Mapping Applicability, Center for Internet Security (last visited June 21, 2023), available at https://www.cisecurity.org/insights/white-papers/cis-controls-cloud-companion-guide-mapping-applicability (earlier version of same resource, in Excel format).

[25] *See, e.g.*, Thales, Best Practices for Cloud Data Protection and Key Management 11 (Jan. 2021), https://cpl.thalesgroup.com/sites/default/files/content/research_reports_white_papers/field_document/2021-02/Best_Practices_in_Cloud-Data-Protection-wp%20%281%29.pdf (presenting via table how responsibilities could be allocated for cloud service provider (CSP) vs customer for different methods of encryption).

own data security enforcement actions.[26]

Because criminals increasingly peddle access to accounts,[27] it is especially important that the Commission give cloud service providers and their enterprise customers adequate incentives to tighten data security measures to prevent this known attack vector from continuing to gain traction. However, even a simple misconfiguration can be sufficient to expose information that should be protected.[28]

We encourage the Commission to emphasize the agreement surrounding what constitutes best practice and the need for clear allocation of responsibilities.

III. Conclusion

EPIC applauds the FTC's inquiry into the state of the Cloud Computing comments. If you have any questions, we remain available and eager to answer any questions.

Respectfully submitted,

/s/ *Ben Winters*	/s/ *Chris Frascella*
Ben Winters	Chris Frascella
Senior Counsel	Law Fellow

Attached:

EPIC's *Generating Harms* Report

[26] *See, e.g.*, EPIC, Disrupting Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystem 181-216 (Nov. 2022), available at https://epic.org/ftc-rulemaking-on-commercial-surveillance-data-security/.

[27] *See, e.g.*, CrowdStrike, 2023 Global Threat Report 9, https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrike2023GlobalThreatReport.pdf (last visited June 21, 2023) ("Access brokers are threat actors who acquire access to organizations and provide or sell this access to other actors, including ransomware operators. The popularity of their services increased in 2022, with more than 2,500 advertisements for access identified — a 112% increase compared to 2021."); Kaspersky ("Malicious actors often breach networks through compromised or weak credentials."); Sam Sabin, Hackers are quickly learning how to breach cloud systems, Axios (Mar. 7, 2023), https://www.axios.com/2023/03/07/hackers-cloud-breaches-cybersecurity.

[28] *See, e.g.*, Brian Krebs, Many Public Salesforce Sites are Leaking Private Data, Krebs on Security (Apr. 27, 2023), https://krebsonsecurity.com/2023/04/many-public-salesforce-sites-are-leaking-private-data/; Top 10 Cloud Security Incidents in 2022, ImmuniWeb (Nov. 29, 2022), https://www.immuniweb.com/blog/top-10-cloud-security-incidents-in-2022.html.