CENTER FOR CYBERSECURITY POLICY AND LAW

May 1, 2026

VIA ELECTRONIC SUBMISSION

RE: DMA. 100209 – Consultation on the Proposed Measures for Google Search Data Sharing (Article 6(11) of the DMA)

I. Summary

The Center for Cybersecurity Policy & Law ("the Center") appreciates the opportunity to submit these comments in response to the preliminary findings in case *DMA.100209 – SP – Alphabet – Article 6(11)*, setting out the proposed data sharing measures that Alphabet must implement pursuant to Article 6(11) of the Digital Markets Act.[1]

The Center is a non-profit organization dedicated to advancing cybersecurity best practices among cybersecurity professionals and industry, with the aim of better protecting public safety. The Center supports regulatory approaches that promote fair competition, while also preserving core security and privacy protections.

The Center is concerned that the European Commission's proposed measures, which require the large-scale, ongoing disclosure of highly granular search data to a broad range of third-party recipients under certain conditions, do not sufficiently account for the applicable security and privacy concerns, and would materially increase public safety concerns and geopolitical risk. These risks are heightened by the breadth and sensitivity of data involved, the diversity of potential recipients, and the increased scope and scale of the cybersecurity threat environment. The Center is further concerned that the proposed technical measures are not sufficient to address these threats.

II. Background on the Preliminary Findings

Article 6(11) of the Digital Markets Act requires "gatekeepers" to provide third-party search engines, upon request, with access on fair, reasonable, and non-discriminatory terms to ranking, query, click, and view data generated by end users on its online search engines.[2] On

[1] European Commission, *Preliminary Measures in Case DMA.100209 (SP – Alphabet – Article 6(11))*, Apr. 16, 2026, [hereinafter "Preliminary Measures"], https://digital-markets-act.ec.europa.eu/document/download/b3aed7f6-c45c-4bfa-b032-b8975a48bb06_en?filename=DMA.100209%20-%20Preliminary%20measures.pdf.

[2] European Parliament & Council of the European Union, *Regulation (EU) 2022/1925 (Digital Markets Act),* Articles 3(1) (defining gatekeeper), 6(11), Sept. 14, 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R1925.

September 5, 2023, the European Commission designated Alphabet Inc. as a gatekeeper, and Google Search a core platform subject to these obligations.[3] In response, Google set up a European Search Dataset Licensing Program, enabling third-party general search engines operating in the European Economic Area (EEA) to license Alphabet's search data, subject to security requirements designed to ensure that the recipient can safeguard the data and is not linked to non-EEA state actors.[4]

The European Commission subsequently opened proceedings designed to further specify Alphabet's obligations under b(11).[5] On April 16, 2026, the European Commission issued its preliminary findings, setting out proposed measures to govern Alphabet's required information sharing.[6] The proposed measures envision extremely broad information sharing, on a daily basis, with a potentially broad number of third-party search providers, and with limited mechanisms to effectively ensure the security of the shared data. These measures raise significant security and privacy concerns.

a. Broad Scope of Data

The proposed measures require Alphabet to provide daily access to multiple categories of highly granular search data to qualifying online search services operating within the European Union (EU) or European Economic Area (EEA). Specifically, the proposal identifies the four principal categories of data:

- **Query data,** including the initial query entered by the user, subsequent refinements, and associated metadata such as language, approximate location, device type, input method, and access point;
- **View data,** including all results displayed in response to a query, together with metadata describing the format, placement, and structure of the search results page;
- **Click data**, including detailed interaction signals such as whether and when a result is clicked, the sequence of interactions, dwell time, return behavior, and other engagement indicators (e.g., scrolling or hovering); and
- **Ranking data**, including information on the ordering and positioning of results, as well as contextual details regarding page layout and presentation.[7]

[3] Digital Markets Act: *Commission Designates Six Gatekeepers*, Sept. 5, 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328.
[4] Google LLC, *About the Google European Search Dataset Licensing Program*, https://developers.google.com/search/help/about-search-data-program.
[5] European Commission, *Commission Opens Proceedings to Assist Google in Complying with Interoperability and Online Search Data Sharing Obligations Under the Digital Markets Act*, Jan. 27, 2026, https://digital-markets-act.ec.europa.eu/commission-opens-proceedings-assist-google-complying-interoperability-and-online-search-data-sharing-2026-01-27_en.
[6] Preliminary Measures, *supra*, n. 1.
[7] Preliminary Measures, *supra,* n. 1, ¶ 4-11.

The proposal further requires that Alphabet provide the data at the record level, and group query, click view, and ranking data from the same user in chronological order.[8] This information creates incredibly granular datasets about user behavior over time.

b. Recipients

The set of potential recipients is broad. It covers all entities providing online search engines in the EU and EEA.[9] Per the preliminary findings, this definition is broad enough to include entities providing AI chatbots with online search engine functionalities, even if the search engine functionalities are just one part of a broader service.[10]

c. Frequency and Methodology of Sharing.

The proposal requires that search data be shared through an Application Programming Interface (API) on par with Alphabet's own frequency of access to the same data—and at least daily.[11]

d. Technical Measures.

The proposal includes certain safeguards intended to mitigate privacy and security risks. These include the required application of anonymization and pseudonymization techniques—implemented through a number of measures, including attribute suppression, allowlist creation, length-based query thresholds, query suppression, metadata generalization, and mini-sessionisation—as well as several contractual obligations, such as prohibitions on re-identification and onward sharing.[12] Alphabet also must require that the third party submit annual reports certifying that, among other things, the recipient has implemented effective technical, organizational, and contractual measures to protect the integrity and confidentiality of the search dataset.[13]

While the inclusion of these safeguards is important, they do not adequately address the security risks identified below. Alphabet appears to bear the burden of monitoring and ensuring that all the requisite security measures are in place. Third-party certifications help, but they do not provide ongoing assurance or monitoring of how entities operate on a daily basis. These concerns are exacerbated by the breadth and sensitivity of information to be shared and the range of potential recipients.

[8] Preliminary Measures, *supra,* n.1, ¶¶ 13, 20.
[9] The preliminary findings adopt the definition of "online search engine" from Article 2(5) of Regulation (EU) 2019/1150 (defining "online search engine" as "a digital service that allows users to input queries in order to perform searches of, in principle, all websites, or all websites in a particular language, on the basis of a query on any subject in the form of a keyword, voice request, phrase or other input, and returns results in any format in which information related to the requested content can be found").
[10] Preliminary Measures, *supra,* n. 1, ¶ 2.
[11] Preliminary Measures, *supra*, n. 1, ¶¶ 15, 17, 20.
[12] Preliminary Measures, *supra*, n. 1, ¶¶ 21–32, 38–52.
[13] Preliminary Measures, *supra*, n. 1, ¶ 66.

III. Cybersecurity, Privacy, and National Security Concerns

Threat Environment

The European Commission's competition-oriented reforms of the digital ecosystem come at a time when the cybersecurity threat landscape is rapidly evolving in both sophistication and scale.

Already, over the past decade, the number and sophistication of cyber-attacks and cyber intrusions have increased exponentially—highlighting the critical importance of strong digital security. Nation-state actors and their proxies are increasingly sophisticated in their ability to infiltrate private and public sector systems, leveraging cyber capabilities for misinformation, espionage, blackmail, and extortion, particularly amid rising geopolitical tension.[14] Among the many recent examples of sophisticated targeted state-sponsored actions: the 2024 reported infiltration of United States telecommunications companies for espionage and disruption;[15] the 2021 Microsoft Exchange breach that compromised tens of thousands of systems in the U.S., granting attackers persistent access to enterprise networks;[16] and the 2009 Operation Aurora attack that targeted major companies, including Adobe, Dow Chemical, Morgan Stanley, and Google, stealing source code and other intellectual property, and accessing personal information of users.[17]

Financially motivated criminals are also a growing threat, with ransomware actors increasing in scope and sophistication. The estimated global cost of cybercrime is projected to rise by over $6.4 trillion between now and 2029, reaching a staggering $15.6 trillion over the next four years.[18] Attackers are adopting more aggressive tactics—including extortion schemes that combine threats to leak stolen information and doxxing (a form of digital abuse that exposes sensitive personal information).[19] Exacerbating the challenges, vulnerabilities in a single app or data transit point can provide an entry point into broad systems. Because applications and data

---

[14] See, e.g., Office of the Director of National Intelligence, *National Counterintelligence Strategy 2024* at 11 (July 30, 2024) ("Cyber threats from nation states and their surrogates remain acute. [Foreign actors] use the cyber domain to undertake their full range of activities, from collection of sensitive information to disruption and destruction of networks to malign foreign influence and monitoring of dissidents. They use technical—and often commercially available—tools to compromise computer networks and mobile and connected devices.").
[15] Chris Jaikaran, Cong. Rsch. Serv., IF12798, *Salt Typhoon Hacks of Telecommunications Companies and Federal Response Implications* at 1 (Jan. 23, 2025), https://crsreports.congress.gov/product/pdf/IF/IF12798.
[16] Dep't of Justice & Cybersecurity and Infrastructure Sec. Agency, *Compromise of Microsoft Exchange Server* at 2 (Mar. 10, 2021), https://www.ic3.gov/CSA/2021/210310.pdf.
[17] Jim Finkle, *Hacker Group in China Linked to Big Cyber Attacks: Symantec*, Reuters (Sept. 17, 2013), https://www.reuters.com/article/technology/hacker-groupin-china-linked-to-big-cyber-attacks-symantec-idUSBRE98G0M7; Ariana Eunjung Cha and Ellen Nakashima, *Google China cyberattack part of vast espionage campaign, experts say*, WASH. POST (Jan. 14, 2010)
[18] Ani Petrosyan, *Estimated Cost of Cybercrime Worldwide 2018-2029*, Statista (Jul. 9, 2024), https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide/.
[19] European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape 2025* at 63 (Oct. 1, 2025) (hereinafter "ENISA Threat Landscape"), https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf (warning of the increasing speed and leverage of intrusions); Office of the Nat'l Cyber Director, *2024 Report on the Cybersecurity Posture of the United States* at 5 (May 2024), https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/05/2024-Report-on-the-Cybersecurity-Posture-of-the-United-States.pdf.

pathways often serve as gateways to interconnected networks, a single flaw can cascade into widespread breaches. The 2020 SolarWinds cyberattack, perpetrated by the Russian Foreign Intelligence Service, exemplifies this risk: attackers compromised a routine software update from a trusted IT management platform, enabling them to infiltrate networks across multiple Fortune 500 companies.[20] This compromise highlights the ways in which a single vulnerability in widely used software can silently propagate through trusted systems, leading to disruptions, far-reaching exposures of data, and ongoing surveillance.[21]

With more entities holding sensitive data, it becomes easier for attackers to breach systems and weaponize data at scale. Foreign adversaries can use access to bulk sensitive data to engage in malicious cyber-enabled activities and malign foreign influence activities and to track and build profiles on specific individuals, including for illicit purposes such as blackmail or espionage.[22]

Developments in artificial intelligence significantly increase these risks. The emergence of increasingly capable frontier models, such as Mythos, is accelerating the ability to find and exploit vulnerabilities, including by automating the discovery of weaknesses that may previously have been considered low risk. These models can ingest and analyze large volumes of code, system logs, and network behavior to automatically surface weaknesses—reducing time, expertise, and resources to carry out complex cyber operations with minimal human input. Tasks that once required highly specialized teams working for weeks or months can now be performed in hours.[23] Of particular concern, Mythos can find hidden flaws via a simple instruction; it can chain multiple small vulnerabilities into a single devastating attack; it can reconstruct source code from deployed software to find exploitable weaknesses; and once inside a network, it can automatically map systems, move laterally, and build custom tools to extract data.[24] Large language models can also be leveraged to craft more convincing phishing emails and automate social engineering activities, among other risks.[25]

Developments in AI also augment privacy risks. By chaining together multiple low-sensitivity data points, even in isolation, AI models can correlate and link what are meant to be de-identified records across data sets. In this way, information that may appear anonymized or low-risk can become identifiable—and highly sensitive—when combined with other data sources.

---

[20] U.S. Gov't Accountability Office, *SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response* (Apr. 22, 2021), https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic.

[21] See also ENISA Threat Landscape *supra n.* 19, at 12 (providing additional examples of adversaries exploiting the digital supply chain, including by compromising software, repositories, or browser extensions).

[22] See Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, 90 Fed. Reg. 1636, 1637–38 (Jan. 8, 2025); see also Department of Justice, *Data Security Program: Implementation and Enforcement Policy Through* July 8, 2025 (Apr. 11, 2025), https://www.justice.gov/opa/media/1396346/dl?inline.

[23] Anthropic's Mythos Moment: *How Frontier AI Is Redefining Cybersecurity*, https://www.weforum.org/stories/2026/04/anthropic-mythos-ai-cybersecurity/.

[24] Frank Ford et al., *Claude Mythos and the AI Cybersecurity Wake-Up Call*, Bain & Co., https://www.bain.com/insights/claude-mythos-and-ai-cybersecurity-wake-up-call/.

[25] See ENISA Threat Landscape, *supra* n. 19, at 14–15 (warning of the ways in which AI tools enable threat activity).

Required Sharing Creates Security and Privacy Risks

The proposed measures introduce significant cybersecurity and privacy risks associated with the large-scale dissemination of sensitive data across a broad and diverse set of third-party recipients.

Required sharing of sensitive datasets creates the risk of breach, misuse, and re-identification, especially in a threat environment where adversaries actively exploit such exposures. As demonstrated by the many breaches of reasonably secure enterprises and government actors discussed above, the underlying assumption that security and data utility can be balanced through simple technical protections is not supported by technical or historical evidence.[26]

These risks are exacerbated by the nature of the data. The preliminary findings require Alphabet to share click, view, and query data at the individual level, with a potentially long list of entities. This is highly sensitive data. Such data reflects what individuals are thinking about, struggling with, or seeking to understand at a particular moment in time. It includes incredibly sensitive information about individuals' personal affiliations, interests, health status and location—creating valuable insights into user behavior, preferences, and patterns of activity.

These risks are compounded as data is distributed across service providers and environments. Each additional holder of the data introduces new potential entry points for malicious actors and new opportunities for de-identification. Even with safeguards in place, each additional point of access introduces new opportunities for de-identification, unauthorized use, interception, tracking, or exploitation.

Data in transit—especially over public or long-distance networks—is particularly exposed to interception, manipulation, and unauthorized access, making secure transmission protocols essential to safeguarding sensitive information.[27] Attackers frequently exploit insecure transfer mechanisms to conduct man-in-the-middle attacks, to spoof recipient addresses, and to take other steps to acquire transiting data.[28] In a distributed system, malicious actors only need to identify the weakest link to access sought after data.[29]

---

[26] Brief of the Center for Cybersecurity Policy & Law as Amicus Curiae Supporting Rehearing, *Epic Games, Inc. v. Google LLC*, No. 24-6256 (9th Cir. 2025) at 6, https://cdn.prod.website-files.com/660ab0cd271a25abeb800460/68222ca2d588da7ff9bfe849_Center%20for%20Cybersecurity%20Amicus%20Brief.FINAL%20(1).pdf.
[27] UK National Cyber Security Centre, *Cloud Security Guidance, Principle 1: Data in Transit Protection* (Nov. 17, 2018), https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles/principle-1-data-in-transit-protection.
[28] UK National Cyber Security Centre, *MOVEit Vulnerability and Data Extortion Incident*, https://www.ncsc.gov.uk/information/moveit-vulnerability.
[29] Brief of the Center for Cybersecurity Policy & Law as Amicus Curiae Supporting Rehearing, *Epic Games, Inc. v. Google LLC*, No. 24-6256 (9th Cir. 2025) at 7, https://cdn.prod.website-files.com/660ab0cd271a25abeb800460/68222ca2d588da7ff9bfe849_Center%20for%20Cybersecurity%20Amicus%20Brief.FINAL%20(1).pdf.

Continuous, high-frequency data sharing further increases the number of technical endpoints that may be targeted. Each endpoint represents a potential vulnerability, heightening the likelihood of unauthorized access, exploitation, or system compromise.

Moreover, once data is shared, there is a diminished ability to control how it is handled, stored, and secured. While recipients are required to be annually certified as meeting baseline requirements, certifying entities do not play a role in day-to-day management of the data. Moreover, while Alphabet can impose contractual requirements on third-party recipients regarding how data is used or protected, Alphabet does not have the means or authority to monitor and ensure compliance. As a result, even those recipients of data that pass third-party reviews are likely to vary significantly in their technical capabilities, security practices, and risk management frameworks. Contractual obligations and baseline security requirements do not ensure consistent implementation or ongoing compliance across all recipients.

Additional Privacy Concerns

The data subject to the mandatory sharing provisions in the preliminary findings includes what the GDPR defines as "special categories of personal data"—to include health-related data and data revealing political opinions, religious beliefs, or philosophical beliefs.[30] GDPR places strict limits on how this type of data can be processed, given the potential harm if it is misused or exposed. The required large-scale sharing of detailed search data appears to conflict with privacy protections laid out in EU law.

The proposed framework also diverges from reasonable user expectations. Users generally understand their search activity to be handled within a defined and trusted service context and rely on providers such as Alphabet to manage their queries with appropriate care. They are far less likely to anticipate that detailed records of their search behavior—including associated interaction data—may be shared on an ongoing basis with multiple third-party entities that are neither visible to them nor subject to their control. This lack of transparency, combined with limited user control over downstream data use, raises concerns regarding fairness, accountability, and user trust.

Proposed Safeguards Are Inadequate

The proposal seeks to address these risks through technical controls and contractual requirements, but these measures are insufficient given the risks.

The risk of data re-identification remains a possibility, even if the anonymization and re-identification procedures are applied. Multiple data points, taken together, can often be used to infer the identity of individuals or to track them across platforms and services, even if certain personal identifiers are not included in the underlying data. Over past decades, there are many examples of large datasets, theoretically de-identified, that are quickly re-identified through the

[30] European Parliament & Council of the European Union, *Regulation (EU) 2016/679 (General Data Protection Regulation)*, Article 9, Apr. 27, 2016, https://gdpr-info.eu/art-9-gdpr/.

use of additional information or datasets.[31] The rapid evolution of data analytics, artificial intelligence, and machine learning techniques heightens the risk of re-identification, as these technologies are increasingly capable of identifying patterns or links that may have been overlooked in traditional anonymization.[32]

Here, the risk is exacerbated because of the scope of data and identity of recipients. De-identified data can be linked with other datasets to reconstruct user identities. For example, a data set that excludes direct identifiers but includes search queries, timestamps, approximate location, and interaction signals could contain a query such as "primary school teacher in Rome recently diagnosed with lung cancer." While each individual element is common, the combination of details may be sufficient to identify an individual, particularly when analyzed using AI systems and in circumstances where data is shared across multiple entities.

Moreover, there are multiple unanswered questions about oversight and enforcement. Alphabet is charged with imposing and enforcing a large list of compliance and related contractual obligations. But it does not have the authority to actively monitor use, nor should it.

Even with unlimited resources, it would be incredibly difficult to monito compliance across such a vast set of entities, particularly where data is integrated with other systems or stored across multiple environments. There is also no guarantee that all entities will adhere to the required standards in practice. As a result, there is a meaningful risk that data may be accessed, combined, or used in ways that are inconsistent with the intended safeguards.

IV. Geopolitical Concerns

The proposed measures also raise broader geopolitical and strategic concerns, particularly in light of the scope of entities that may be eligible to receive search data. As mentioned, the definition of qualifying services extends to AI chatbots and others that meet the definition of online search engine. The sharing requirements laid out in the preliminary findings do not account for ownership structure, jurisdictional affiliation, or the broader data ecosystem in which those entities operate.

In practice, this framework may result in access being granted to a wide swath of entities that, while operating within the EU or EEA, are headquartered elsewhere or subject to foreign ownership or control. This raises important concerns regarding oversight and accountability. Data shared pursuant to the DMA may become subject to legal regimes and governmental access frameworks outside the EU's regulatory perimeter. In such cases, third-party recipients may be required to comply with foreign legal obligations that could compel access to or disclosure of the data. As a result, protections afforded under EU law may not fully extend to the

[31] Luc Rocher, Julien M. Hendrickx & Yves-Alexandre de Montjoye, *Estimating the Success of Re-identifications in Incomplete Datasets Using Generative Models* at 10, Nature Commc'ns 3069, https://www.nature.com/articles/s41467-019-10933-3.

[32] Brief of the Center for Cybersecurity Policy & Law as Amicus Curiae Supporting Rehearing, *Epic Games, Inc. v. Google LLC*, No. 24-6256 (9th Cir. 2025) at 9, https://cdn.prod.website-files.com/660ab0cd271a25abeb800460/68222ca2d588da7ff9bfe849_Center%20for%20Cybersecurity%20Amicus%20Brief.FINAL%20(1).pdf.

downstream handling of the data, particularly where enforcement mechanisms are fragmented across jurisdictions.

Beyond third-party certifications, the proposal does not adequately address the potential for data to be used beyond the immediate purpose of supporting search services. Access to large-scale, high-quality search data may create incentives for recipients to use such data for other purposes, including the development or refinement of artificial intelligence systems or other data-driven capabilities. These downstream uses may be difficult to monitor in practice and may extend beyond the intended scope of the data-sharing obligation.

V. Conclusion

The Center is concerned that the preliminary findings will require extensive sharing of highly sensitive data, without sufficient security and privacy protections. The Center urges that the Commission revise the findings to account for the current threat environment, narrow the scope and scale of data sharing, place additional security controls on the data recipients, establish an effective monitoring and enforcement system, and limit recipients to those that do not have ties to state actors outside of the European Union.

The Center appreciates the Commission's consideration of these comments and welcomes continued engagement on these issues. Should you have any questions or require additional information, please do not hesitate to contact Jennifer Daskal, jdaskal@venable.com or Ari Schwartz, acschwartz@venable.com.