Submission to the European Commission on the proposed measures for interoperability with Google Android (Article 6(7) of the DMA)

Dr Christophe Carugati

The Commission's measures on Google's interoperability with AI services require safeguards to preserve innovation, protect end users and app developers from privacy and security risks, and ensure implementation through a forum.

Introduction

The European Commission is seeking stakeholder feedback until 13 May 2026 on its proposed interoperability measures for the Alphabet-owned Google Android operating system ("Google Android") under Article 6(7) of the Digital Markets Act (Regulation (EU) 2022/1925, DMA) ("the consultation")[1].

Under Article 6(7), Google Android must provide third-party software and hardware providers with effective, free-of-charge interoperability with the same software and hardware features that Google accesses or controls. Google may impose only measures that are strictly necessary and proportionate to protect the integrity of its operating system, software, and hardware.

The consultation forms part of the ongoing specification proceeding concerning Alphabet's interoperability obligations under Article 8(2) of the DMA, which the Commission opened on 27 January 2026[2]. The proceeding seeks to clarify how

[1] DMA.100220 – Consultation on the Proposed Measures for Interoperability with Google Android (Article 6(7) of the DMA (accessed 1st May 2026). Available at: https://digital-markets-act.ec.europa.eu/dma100220-consultation-proposed-measures-interoperability-google-android-article-67-dma_en

[2] Commission Opens Proceedings to Assist Google in Complying with Interoperability and Online Search Data Sharing Obligations Under the Digital Markets Act, *European Commission*, 27 January 2026 (accessed 24 April 2026). Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_26_202

interoperability requirements can effectively promote contestability and fairness in the provision of Artificial Intelligence ("AI") services on Google Android.

This marks the third specification proceeding under Article 6(7) of the DMA. The first two proceedings, closed in March 2025, concerned connected devices and interoperability request procedures involving Apple[3]. The present proceeding focuses specifically on AI in light of rapid developments in the sector and the Commission's broader consultation on the DMA's applicability to AI[4].

Against this backdrop, the Commission proposes measures requiring access to several hardware and software features. These measures include:

- features for invocation, enabling third-party services to launch through system access points such as the home interface, navigation controls, and hotword detection (Section 1 of the Annex to the consultation);
- features for context, allowing access to relevant app data stored on-device and contextual information, such as ambient data from device sensors (section 2);
- features enabling actions across apps and operating system functions (Section 3);
- features governing access to resources, including use of on-device models (ODMs) and background execution (Section 4); and
- horizontal measures applicable across all features, covering implementation throughout the Google Android ecosystem, user consent, integrity safeguards, eligibility of beneficiaries, equal effectiveness, free-of-charge requirement, documentation and Application Programming Interfaces ("APIs"), testing and technical assistance, future updates and functionalities, reporting obligations, and waiver (Section 5).

These measures seek to preserve the DMA's objectives amid rapid developments in the AI sector. The sector currently exhibits strong competitive dynamics and sustained innovation and investment from both established firms and new entrants. Investments in software and hardware are driving the rapid release of new AI models, including ODMs, as well as AI-powered services and products. Alphabet alone announced approximately 100 new features in 2025, most of which related to AI functionality in its products and

[3] DMA.100203 *Apple – Operating systems – iOS – Article 6(7) – SP – Features for Connected Physical Devices*, 19 March 2025; DMA.100204 *SP - Apple - Article 6(7) – process*, 19 March 2025.

[4] Consultation on the First review of the Digital Markets Act, *European Commission* (accessed 28 April 2026). Available at: https://digital-markets-act.ec.europa.eu/consultation-first-review-digital-markets-act_en

services. These include Circle to Search on selected Android devices and the development of its Gemini models[5].

While these developments stimulate innovation, they also create new privacy and security risks. In particular, AI agents that perform tasks on behalf of users require extensive access to software, hardware, and data. Such access may compromise system integrity and expose users to significant privacy and security harms. For example, the Dutch data protection authority has warned of major security risks associated with AI agents such as OpenClaw, including the use of hidden commands that can extract sensitive data[6].

Against this background, the consultation raises three main issues. First, the proposed measures may undermine innovation by reducing Alphabet's ability to develop innovative features, weakening the incentives of both Alphabet and third-party hardware and software providers to innovate, and imposing potentially disproportionate free-of-charge obligations, such as for technical assistance. These concerns call for safeguards that preserve incentives to innovate and invest.

Second, the proposed measures raise significant privacy and security concerns. Protecting system integrity alone may not be sufficient to protect end users and application developers from the new risks associated with AI agents. These risks call for safeguards that directly protect users against privacy and security harms.

Third, the proposed measures raise important implementation challenges across the Google Android ecosystem. Alphabet must ensure implementation across all Android devices, yet it may lack both the technical and contractual means to enforce it with device manufacturers. These challenges call for ensuring implementation through a dedicated Android Interoperability Implementation Forum.

[5] Molly McHugh-Johnson, 100 Things We Announced at I/O, *Google Blog,* 21 May 2025 (accessed 1st May 2026). Available at: https://blog.google/innovation-and-ai/products/google-io-2025-all-our-announcements/

See also, Harsh Kharbanda, See the Whole Picture and Find the Look with Circle to Search, *Google Blog,* 25 February 2026 (accessed 1st May 2026). Available at: https://blog.google/products-and-platforms/products/search/circle-to-search-february-2026/

[6] AP Warns of Major Security Risks with AI Agents Like Openclaw, *Autoriteit Persoonsgegeven*, 12 February 2026 (accessed 1st May 2026). Available at: https://www.autoriteitpersoonsgegevens.nl/en/current/ap-warns-of-major-security-risks-with-ai-agents-like-openclaw

This submission examines these three main issues raised in the consultation through a thematic framework focused on innovation, privacy and security, and implementation across the Google Android ecosystem. Each section begins with a critical assessment of the proposed measures and concludes with specific policy recommendations.

Innovation

The Commission proposes that Alphabet provide third parties with access to the same Google Android software and hardware features, and all related functionalities, that Alphabet makes available to its own services, in a manner that is equally effective (paras. 3, 11, 23, 31, 41, 50, 59, 68, 77, 87, 96, 105, and 114 of the Annex to the consultation). For example, Alphabet must provide access to hardware features such as the Long-Press Home (LPH) and Long-Press Navigation Handle (LPNH) contextual invocation features, which enable functionalities such as Circle to Search (para. 2). Alphabet must also provide access to software features closely integrated into commercial products, such as system-level ODMs, which support Gemini Nano ODMs (para. 100).

In addition, Alphabet must provide, free of charge, the interoperability solutions and measures necessary to achieve effective interoperability with these hardware and software features, regardless of the beneficiary, application, service, product, or use case. Alphabet must not impose indirect charges for any of these measures (Section 5.6). The required interoperability solutions and measures include documentation APIs (Section 5.7). Alphabet must also provide third parties with reasonable technical assistance, free of charge, to facilitate implementation and ensure effective interoperability (Section 5.8).

Moreover, Alphabet must ensure effective interoperability for future updates and functionalities insofar as they are available to Alphabet's own services or hardware (paras. 6, 18, 26, 36, 45, 54, 63, 72, 82, 91, 100, 109, and 118, and Section 5.9). In particular, Alphabet must make interoperability solutions available no later than the moment when the relevant feature becomes accessible to any Alphabet service or hardware on the same Google Android mobile device (para 150).

Critical Analysis

The proposed measures could materially affect Alphabet's ability and incentive to develop and deploy innovative hardware and software features on Google Android.

First, the measures may constrain Alphabet's ability to innovate. Requiring innovative features to interoperate with third-party services and hardware obliges Alphabet to develop interoperability solutions before launching those features. Designing and implementing such solutions often involves complex, resource-intensive, and time-consuming engineering work, which may delay or, in some cases, prevent the rollout of innovative functionalities. For example, Apple reportedly delayed the launch of its Live Translation feature because developing interoperability solutions required additional engineering work to ensure that user data was processed on-device and remained inaccessible to third parties. Apple has also delayed the launch of its iPhone Mirroring feature on non-Apple devices, reportedly because it has not yet identified a sufficiently secure interoperability solution[7]. Accordingly, where interoperability solutions prove technically complex or infeasible, Alphabet may delay the rollout of innovative features in Europe or refrain from launching them altogether.

Second, the proposed simultaneity requirement may weaken incentives to innovate. By requiring interoperability solutions to become available at the same time as Alphabet's own services and hardware, the measures would require Alphabet to share the benefits of innovation with third parties immediately upon launch. This approach may undermine the contestability and appropriability principles identified by Professor Carl Shapiro as key drivers of innovation incentives[8].

Under the contestability principle, "*the prospect of gaining or protecting profitable sales by providing greater value to customers spurs innovation*." If third parties can immediately replicate or access the same functionalities, the innovator cannot differentiate its products or services by offering superior value to customers. This reduces the incentive to undertake risky and costly innovation investments. At the same time, third parties may have weaker incentives to innovate independently if they can rely on immediate access to another firm's innovations. This dynamic could encourage free-riding rather than entry through differentiated innovation, thereby undermining the DMA's objective of promoting contestability.

Similarly, under the appropriability principle, "*increased appropriability spurs innovation*." Firms invest in innovation when they can appropriate at least part of the value generated by their investments. Immediate interoperability obligations may prevent Alphabet from

[7] The Digital Markets Act's Impacts on EU Users, *Apple*, 24 September 2025 (accessed 5 May 2026). Available at: https://www.apple.com/newsroom/2025/09/the-digital-markets-acts-impacts-on-eu-users/

[8] Carl Shapiro, Competition and Innovation 7 Did Arrow Hit the Bull's Eye?, *NBER Chapters, in: The Rate and Direction of Inventive Activity Revisited,* 2011. Available at: https://faculty.haas.berkeley.edu/Shapiro/arrow.pdf

enjoying any temporary competitive advantage from its innovations, as third parties could rapidly imitate or replicate new functionalities. This may reduce incentives to innovate for both Alphabet, as imitation is immediate, and third parties, as it can simply offer an imitation. As Professor Shapiro argues, firms cannot offer superior value to consumers in environments where imitation becomes immediate and effective, thereby undermining contestability[9]. Accordingly, the proposed simultaneity requirement risks reducing dynamic competition and long-term innovation incentives.

Third, the Commission's interpretation of the free-of-charge requirement may exceed what Article 6(7) of the DMA requires and may prove disproportionate. A literal reading of Article 6(7) provides that "*[Alphabet] shall allow providers of services and providers of hardware, free of charge, effective interoperability with, and access for the purposes of interoperability to, the same hardware and software features […]*". The sentence "*free of charge*" appears to apply to interoperability solutions itself, rather than to the underlying commercial products or services into which those features are integrated. For example, Alphabet currently charges third parties for access to certain Gemini models through paid APIs on a usage basis[10].

Ensuring effective interoperability necessarily requires developing and maintaining documentation and APIs. However, these processes require substantial engineering resources and ongoing maintenance. For example, following the Commission's interoperability decision concerning Microsoft in 2004, Microsoft stated that "*hundreds of Microsoft employees and contractors have worked for more than 30,000 hours to create over 12,000 pages of detailed technical documents that are available for license today.*[11]" Given these potentially significant compliance costs, requiring Alphabet to provide and maintain interoperability documentation and APIs at no cost may be disproportionate.

Similarly, requiring Alphabet to provide technical assistance free of charge may go beyond what effective interoperability strictly requires. Technical assistance constitutes a separate customer service that demands significant human resources, expertise, and time. Mandating such assistance without compensation may therefore impose disproportionate compliance burdens that exceed the DMA's text.

---

9 *Ibid.*

10 Gemini Developer API pricing, *Google* (accessed 6 May 2026). Available at: https://ai.google.dev/gemini-api/docs/pricing

11 Microsoft Refutes European Commission Case, Microsoft, *Microsoft Blog*, 15 February 2006 (accessed 6 May 2026). Available at: https://news.microsoft.com/source/2006/02/15/microsoft-refutes-european-commission-case

Finally, the Commission's interpretation requiring simultaneous access to present and future innovative features may go beyond the DMA's wording. Article 6(7) requires "*effective interoperability […] to, the same hardware and software features […] as are available to services or hardware provided by [Alphabet].*" The sentence "*as are available*" primarily concerns the substantive scope of access, namely, which features must be interoperable, rather than the precise timing of interoperability. Interoperability may remain fully effective even if the interoperability solution becomes available after the innovator launches the feature. Accordingly, the DMA does not appear to mandate simultaneous access as a matter of law.

Policy Recommendations

The Commission should avoid imposing a strict simultaneity requirement in order to preserve the ability and incentives for innovation. Instead, it should permit Alphabet to provide interoperability solutions after a reasonable period (e.g., a year) following the launch of a new feature. This approach would preserve both Alphabet's and third-party providers' ability and incentive to invest in innovation, while allowing sufficient time to develop secure and effective interoperability solutions.

The Commission should also consider preventing third parties from using interoperability access to develop competing products or services. In this regard, it could draw inspiration from the Data Act (Regulation (EU) 2023/2854, DA), which requires data sharing for connected devices while restricting third parties from using shared data to develop competing connected products, allowing their use for developing related services to preserve downstream innovation incentives (Article 6(2)(e) and Recital 32). A similar approach could balance interoperability obligation with incentives to innovate under the DMA.

Finally, the Commission should not require Alphabet to provide access to commercial software features, documentation, APIs, and technical assistance entirely free of charge. To ensure proportionality, the Commission should allow Alphabet to recover at least marginal compliance costs associated with developing, maintaining, and supporting interoperability solutions.

Privacy and Security

The Commission proposes that Alphabet provide access to software and hardware features relating to context (Section 2), including measures for proactive suggestions that would allow application developers to donate, among other things, app data to third parties (Section 2.2).

The Commission further requires Alphabet to implement measures for context-aware intelligence that would grant third-party providers access to the user's physical context, such as ambient data collected through sensors, including cameras, to the user's digital context, including device audio, data from apps, services, or the operating system, and global access to app data and actions stored on-device (Section 2.3).

In addition, the Commission requires Alphabet to implement measures enabling third-party providers to access ambient data (Section 2.4).

For all three categories of measures, the Commission permits Alphabet to implement technical safeguards in line with the principles of process isolation, encryption, anonymous and aggregated telemetry, and user control, provided that these safeguards rely on transparent, objective, precise, and non-discriminatory conditions that also apply to Alphabet's own services and hardware (paras. 35, 44, and 53).

The Commission also requires Alphabet to implement measures relating to actions across apps and operating system functions. These measures would permit third-party providers to take actions within apps (Section 3.1), control apps on behalf of users (Section 3.2), write and read alongside Alphabet's own apps (Section 3.3), and interact and integrate with operating system functionalities on behalf of users (Section 3.4).

The Commission permits Alphabet to implement technical measures to protect end users, including system-level prompts, to ensure that third parties access these functionalities only after user consent. Such measures must rely on transparent, objective, precise, and non-discriminatory conditions that equally apply to Alphabet's own services and hardware (Section 5.2).

Finally, the Commission allows Alphabet to adopt strictly necessary and proportionate measures to ensure that interoperability does not compromise the integrity of the

operating system or hardware and software features. These measures must be duly justified and based on transparent, objective, precise, and non-discriminatory conditions that also apply to Alphabet's own services and hardware (Section 5.3).

Critical Analysis

The proposed measures raise significant privacy and security concerns for end users and application developers.

From a privacy perspective, the proposed access measures for proactive suggestions and context-aware intelligence would give third-party providers access to highly sensitive personal data. The Commission seeks to mitigate these risks through user consent requirements and technical safeguards such as encryption.

However, user consent alone does not sufficiently protect privacy. Although the Commission allows Alphabet to ensure that access occurs only after the user provides consent, consent-based prompts cannot prevent misuse once access has been granted. A malicious third-party provider could use the data for purposes unrelated to proactive suggestions or context-aware intelligence, including commercial resale. User consent, therefore, remains necessary but insufficient as a privacy safeguard.

Similarly, the technical safeguards permitted by the Commission address only part of the privacy risk. The proposed principles—process isolation, encryption, anonymous and aggregated telemetry, and user control—help reduce risks such as unauthorised third-party access to data. However, they do not adequately address misuse by authorised third parties. For example, they do not prevent authorised providers from repurposing decrypted data for unauthorised uses or from re-identifying anonymous data. Accordingly, while the proposed technical safeguards remain necessary, they do not by themselves provide sufficient protection for user privacy.

The proposed measures also create significant security risks. Granting third-party providers extensive control over apps and operating system functionality introduces new vulnerabilities associated with AI agents, including prompt-injection attacks. In such attacks, malicious instructions manipulate the AI agent into performing unintended actions, such as disclosing or exfiltrating sensitive data.

The Commission's framework currently permits Alphabet to adopt safeguards only to the extent necessary to protect the integrity of the operating system and hardware and software features. However, this interpretation may be too narrow to address the specific security risks posed by AI agents.

Indeed, in its specification proceeding concerning Apple's connected devices, the Commission interpreted integrity as a property of services and functionalities, rather than as a concept primarily aimed at protecting end users[12]. In that context, the Commission acknowledged that integrity measures may indirectly protect user privacy and security, but only where necessary to prevent the manipulation of security and privacy controls without the user's authorisation[13].

This interpretation, which focuses primarily on system integrity rather than user protection, may constrain Alphabet's ability to implement broader safeguards against AI-agent risks such as prompt injection. In many cases, prompt injection attacks target users directly through systems that technically continue to function as intended. Accordingly, a narrow integrity-based approach may fail to provide adequate protection against emerging AI-specific security threats.

Moreover, the proposed measures may fail to adequately account for the interests of application developers. By enabling third-party providers to act across apps and operating system functionalities, the Commission effectively permits third parties to execute tasks within apps without requiring app developers' authorisation. The proposed framework does not currently allow app developers to permit or deny such access.

Recent developments in the United States illustrate these concerns. Amazon has reportedly blocked several AI agents, such as the one developed by Perplexity. In a lawsuit against Perplexity, Amazon alleged that Perplexity lacked authorisation to execute tasks on Amazon's platform and argued that such AI agents posed security risks by accessing private customer accounts and posed challenges for Amazon's advertising business, as they generate non-human ad traffic[14]. These concerns demonstrate that the absence of

[12] DMA.100203, para. 103.

[13] *Ibid*, para. 106.

[14] Annie Palmer, Amazon Wins Court Order to Block Perplexity's AI Shopping Agent, *CNBC*, 10 March 2026 (accessed 7 May 2026). Available at: https://www.cnbc.com/2026/03/10/amazon-wins-court-order-to-block-perplexitys-ai-shopping-agent.html

an authorisation framework may inadequately protect application developers' legitimate commercial and security interests.

Finally, the proposed measures may overlap with obligations under the Cyber Resilience Act (Regulation (EU) 2024/2847, CRA). The CRA imposes cybersecurity obligations on manufacturers of products with digital elements (Article 13), which may conflict with interoperability obligations requiring broad third-party access despite cybersecurity risks. Without further clarification, the interaction between the DMA and the CRA may create legal uncertainty for Alphabet and lead to inconsistencies across regulatory regimes.

Policy Recommendations

The Commission should permit broader privacy and security safeguards to address the risks associated with AI agents. In particular, it should adopt a broader interpretation of integrity measures that encompasses risks directly affecting end users, rather than limiting integrity solely to the protection of system functionalities and service properties.

The Commission should also establish an authorisation framework that allows application developers to permit or restrict third-party providers from executing tasks within their apps. Such a framework would better protect developers' commercial interests, preserve platform security, and reduce the risk of unauthorised automated access.

Finally, the Commission should clarify the relationship between the proposed DMA measures and the CRA to ensure legal certainty and regulatory consistency. To achieve this, the Commission should closely cooperate with the European Data Protection Board ("EDPB") and the European Union Agency for Cybersecurity ("ENISA") to assess and address privacy and cybersecurity risks arising from the proposed interoperability measures.

Implementation Across the Google Android Ecosystem

The Commission proposes that Alphabet implement the proposed interoperability measures across all devices running Google Android, including both Alphabet's own devices and devices manufactured by third-party original equipment manufacturers ("OEMs"), such as Samsung.

To this end, the Commission requires Alphabet to implement the proposed measures on all relevant devices through technical and contractual means, provided that the relevant feature exists on the device and that the device continues to receive Android Open Source Project ("AOSP"), Google Play system, or Google system services updates (Section 5.1).

In several instances, the Commission imposes explicit obligations on Alphabet regarding OEMs. For example, Alphabet must ensure that third-party apps do not face access restrictions requiring pre-installation, privileged permissions, or other OEM-controlled restrictions (para. 90). In addition, where Alphabet allows OEMs to customise or otherwise modify access to hardware resources or background execution capabilities for ODMs or software to implement such models, Alphabet must ensure that such customisations comply with all proposed measures (para. 108). Similarly, if Alphabet permits OEMs to customise background execution rules, Alphabet must ensure that those rules also comply with the proposed measures (para. 117).

The Commission also imposes indirect obligations on OEMs. For instance, the proposed measures governing ODM implementation require Alphabet and OEMs to provide third parties with access to hardware resources necessary to install, run, and use ODMs, including CPU, GPU, NPU, and RAM resources, as well as RAM residency (Section 4.2).

Critical Analysis

The proposed measures would significantly affect how both Alphabet and OEMs manage their versions of Google Android, their hardware and software resources, and their commercial relationships with third parties.

First, the measures may constrain Alphabet and OEMs' ability to customise Google Android. At present, OEMs retain considerable flexibility in adapting Google Android to differentiate their products and services. However, interoperability obligations relating to areas such as background execution rules could limit that flexibility by imposing harmonised requirements across devices. This may reduce product differentiation among Google Android mobile devices.

Second, the proposed measures may affect the management and performance of hardware and software resources. Alphabet and OEMs currently retain discretion over how they allocate hardware resources and optimise software functionalities on their

devices. Obligations requiring access to hardware resources for third-party ODMs, including CPU, GPU, NPU, and RAM, could restrict their ability to develop and improve proprietary functionality, such as AI models and services, as they cannot use these resources optimally. These obligations may also affect overall device performance, such as system responsiveness. As a result, the measures could negatively affect product and service quality, as well as hardware performance across devices.

Third, the measures may interfere with existing and future commercial relationships that Alphabet and OEMs have with third parties. For example, obligations regarding ODM interoperability could affect strategic commercial partnerships between OEMs and model developers, such as collaborations between Alphabet and Samsung to deploy Gemini functionalities on certain Samsung devices[15]. Other measures, including interoperability obligations concerning always-on hotword detection, would require extensive technical coordination between third-party software developers and OEMs. As the Commission itself acknowledges, implementing hotword detection capabilities depends on hardware-specific components such as digital signal processors ("DSPs"), which vary across devices. Consequently, effective implementation would require close collaboration between OEMs and third-party providers, potentially limiting OEMs' commercial discretion and operational autonomy.

Moreover, the Commission's proposed requirement that Alphabet implement the measures on all Android devices through technical and contractual means presents practical limitations.

From a technical perspective, implementation feasibility depends heavily on device-specific characteristics, including the availability and configuration of relevant hardware components such as DSPs. Even where the necessary hardware exists, effective implementation would require substantial cooperation between OEMs and third-party providers. Alphabet may lack the technical and operational control necessary to intervene in such cooperation, as it does not directly control the relevant hardware or software environment.

From a contractual perspective, implementation depends on existing and future agreements between Alphabet and OEMs. Although Alphabet could seek to amend contractual arrangements to require compliance with the proposed measures, OEMs may

[15] Samsung and Google Cloud Join Forces to Bring Generative AI to Samsung Galaxy S24 series, *Samsung*, 17 January 2024 (accessed 8 May 2026). Available at: https://news.samsung.com/global/samsung-and-google-cloud-join-forces-to-bring-generative-ai-to-samsung-galaxy-s24-series

not necessarily accept such amendments. Even when OEM agrees to contractual amendments, Alphabet would still face practical limits in ensuring effective implementation, particularly where interoperability obligations intersect with independent commercial relationships between OEMs and third-party providers. In many cases, Alphabet would remain a third party to those relationships and would lack the authority to impose operational or technical conditions directly.

Policy Recommendations

Rather than requiring Alphabet to implement the measures, the Commission should establish a dedicated Android Interoperability Implementation Forum to ensure effective and coordinated implementation across the Google Android ecosystem.

The Forum should bring together the Commission, acting as chair, alongside Alphabet, a representative group of OEMs, and representatives of third-party hardware and software providers. The EDPB and ENISA should participate as observers with the ability to issue non-binding opinions where implementation issues raise data protection or cybersecurity concerns.

The Forum should operate through three dedicated working groups.

A technical working group should assess Alphabet's proposed interoperability solutions before implementation. This process would allow OEMs to raise technical feasibility concerns and enable third-party providers to identify potential interoperability gaps or implementation barriers.

A compliance working group should monitor the effective implementation of the measures, taking into account Alphabet's reporting obligations and stakeholder feedback. This group could facilitate greater transparency and identify implementation issues at an early stage.

Finally, a dispute resolution working group should provide a structured mechanism for addressing implementation disputes raised by OEMs or third-party providers. The group should issue non-binding findings that the Commission may consider when exercising its monitoring and enforcement powers under the DMA.

About

Digital Competition

Digital Competition (https://www.digital-competition.com/) is dedicated to promoting digital and competition policies that foster innovation. We bring together legal, economic, and policy expertise to deliver cutting-edge research, training, strategic advice, and high-impact regulatory intelligence.

Led by Dr Christophe Carugati, with a decade of deep expertise in digital and AI markets, we address the most pressing challenges in the rapidly evolving digital and competition policy landscape, impartially, rigorously, and with a commitment to actionable recommendations.

Google provided financial support for this submission. The views, analyses, and recommendations are solely those of the author, not those of his clients, which also include Apple and Amazon.

This paper is part of our Digital Competition Regime Hub (https://www.digital-competition.com/digitalcompetitionregime). We conduct research on the design, implementation, and enforcement of digital competition regimes worldwide, from the EU DMA to the UK DMCCA.

Contact us for service, membership, training, or press inquiries.

Dr. Christophe Carugati

Dr. Christophe Carugati (christophe.carugati@digital-competition.com) is the founder of Digital Competition. He is a renowned and passionate expert on digital and competition issues with a strong reputation for doing impartial, high-quality research. After his PhD in law and economics on Big Data and Competition Law, he is an ex-affiliate fellow at the economic think tank Bruegel and an ex-lecturer in competition law and economics at Lille University.